OpenShift Container Platform 4.15

容器迁移工具套件（MTC）

迁移到 OpenShift Container Platform 4

Last Updated: 2024-07-24

OpenShift Container Platform 4.15 容器迁移工具套件（MTC）

迁移到 OpenShift Container Platform 4

法律通告

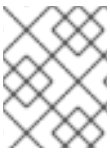
摘要

本文档提供在 OpenShift Container Platform 4 集群间迁移有状态应用程序工作负载的说明。

目录

第 1 章 关于 MIGRATION TOOLKIT FOR CONTAINERS（MTC）

MTC（Migration Toolkit for Containers）可让您按照命名空间将有状态应用程序工作负载在不同 OpenShift Container Platform 4 集群间进行迁移。



注意

如果要从 OpenShift Container Platform 3 迁移，请参阅关于从 OpenShift Container Platform 3 迁移到 4以及在 OpenShift Container Platform 3 上安装旧的 MTC Operator。

您可以使用状态迁移，在同一集群或不同集群间迁移应用程序。

MTC 提供了一个基于 Kubernetes 自定义资源的 web 控制台和 API，可帮助您控制迁移并最小化应用程序停机时间。

MTC 控制台默认安装在目标集群中。您可以配置 MTC Operator，以便在远程集群中安装控制台。

有关以下主题的详情，请参阅高级迁移选项：

- 使用迁移 hook 和 MTC API 自动迁移。
- 配置迁移计划以排除资源，支持大规模迁移，并为直接卷迁移启用自动 PV 大小调整。

1.1. 术语

表 1.1. MTC 术语

术语	定义
源集群	从中迁移应用程序的集群。
目标集群[1]	将应用程序迁移到的集群。
复制软件仓库	用于在间接迁移过程中复制镜像、卷和 Kubernetes 对象的对象存储，或者用于直接卷迁移或直接镜像迁移期间 Kubernetes 对象的对象存储。 复制存储库必须可以被所有集群访问。
主机集群	运行 **migration-controller** pod 和 Web 控制台的集群。主机集群通常是目标集群，但这不是必需的。 主机集群不需要公开的 registry 路由来直接迁移镜像。
远程集群	远程集群通常是源集群，但这不是必需的。 远程集群需要一个包含 **migration-controller** 服务帐户令牌的 **Secret** 自定义资源。 远程集群需要一个公开的安全 registry 路由来直接迁移镜像。
间接迁移	镜像、卷和 Kubernetes 对象从源集群复制到复制存储库，然后从复制存储库复制到目标集群。

术语	定义
直接卷迁移	持久性卷直接从源集群复制到目标集群。
直接镜像迁移	镜像直接从源集群复制到目标集群。
阶段迁移	在不停止应用程序的情况下，数据将复制到目标集群。 多次运行阶段迁移会缩短迁移的持续时间。
剪切迁移	应用在源集群中停止，其资源迁移到目标集群。
状态迁移	通过将特定的持久性卷声明复制到目标集群来迁移应用程序状态。
回滚迁移	回滚迁移会回滚一个已完成的迁移。

[1] 在 MTC web 控制台中称为 *目标集群*。

1.2. MTC 工作流

您可以使用 MTC web 控制台或 Kubernetes API 将 Kubernetes 资源、持久性卷数据和内部容器镜像迁移到 OpenShift Container Platform 4.15。

MTC 迁移以下资源：

- 在迁移计划中指定的命名空间。
- 命名空间范围的资源：当 MTC 迁移命名空间时，它会迁移与该命名空间关联的所有对象和资源，如服务或 Pod。另外，如果一个资源在命名空间中存在但不在集群级别，这个资源依赖于集群级别存在的另外一个资源，MTC 会迁移这两个资源。
  例如，安全性上下文约束（SCC）是一个存在于集群级别的资源，服务帐户（SA）是存在于命名空间级别的资源。如果 MTC 迁移的命名空间中存在 SA，MTC 会自动找到链接到 SA 的所有 SCC，并迁移这些 SCC。同样，MTC 会迁移链接到命名空间持久性卷声明的持久性卷。

  注意

  根据资源，可能需要手动迁移集群范围的资源。

- 自定义资源 (CR) 和自定义资源定义 (CRD)：MTC 在命名空间级别自动迁移 CR 和 CRD。

使用 MTC Web 控制台迁移应用程序涉及以下步骤：

1. 在所有集群中安装 MTC Operator。
   您可以在有限的或没有互联网访问的受限环境中为 Containers Operator 安装 Migration Toolkit。源和目标集群必须可以在相互间进行访问，而需要可以访问 registry 的镜像（mirror）.
2. 配置复制存储库，这是 MTC 用来迁移数据的中间对象存储。
   源和目标集群必须有对复制仓库的不受限制的网络访问权限。如果使用代理服务器，您必须将其配置为允许复制仓库和集群间的网络流量。
3. 在 MTC web 控制台中添加源集群。

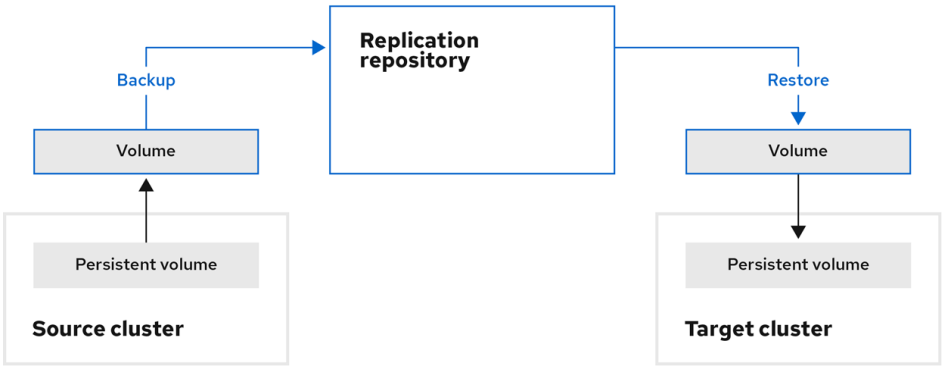
4. 在 MTC web 控制台中添加复制存储库。

5. 创建迁移计划，包含以下数据迁移选项之一：

   - **Copy**：MTC 将数据从源集群复制到复制存储库，再从复制存储库把数据复制到目标集群。

     注意

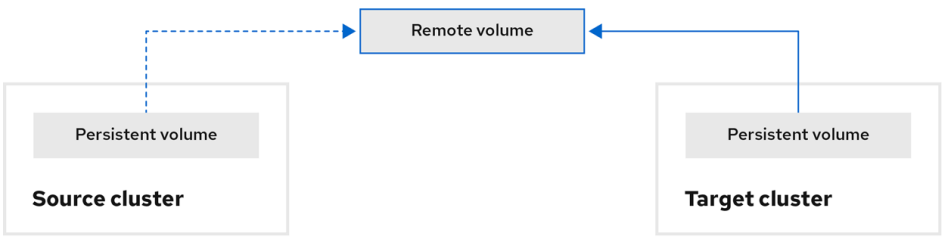
     如果您使用直接镜像迁移或直接卷迁移，则镜像或卷会直接从源集群复制到目标集群。



   - **Move**：MTC 从源集群中卸载一个远程卷（例如 NFS），在目标集群上创建一个指向这个远程卷的 PV 资源，然后在目标集群中挂载远程卷。在目标集群中运行的应用程序使用源集群使用的同一远程卷。远程卷必须可以被源集群和目标集群访问。

     注意

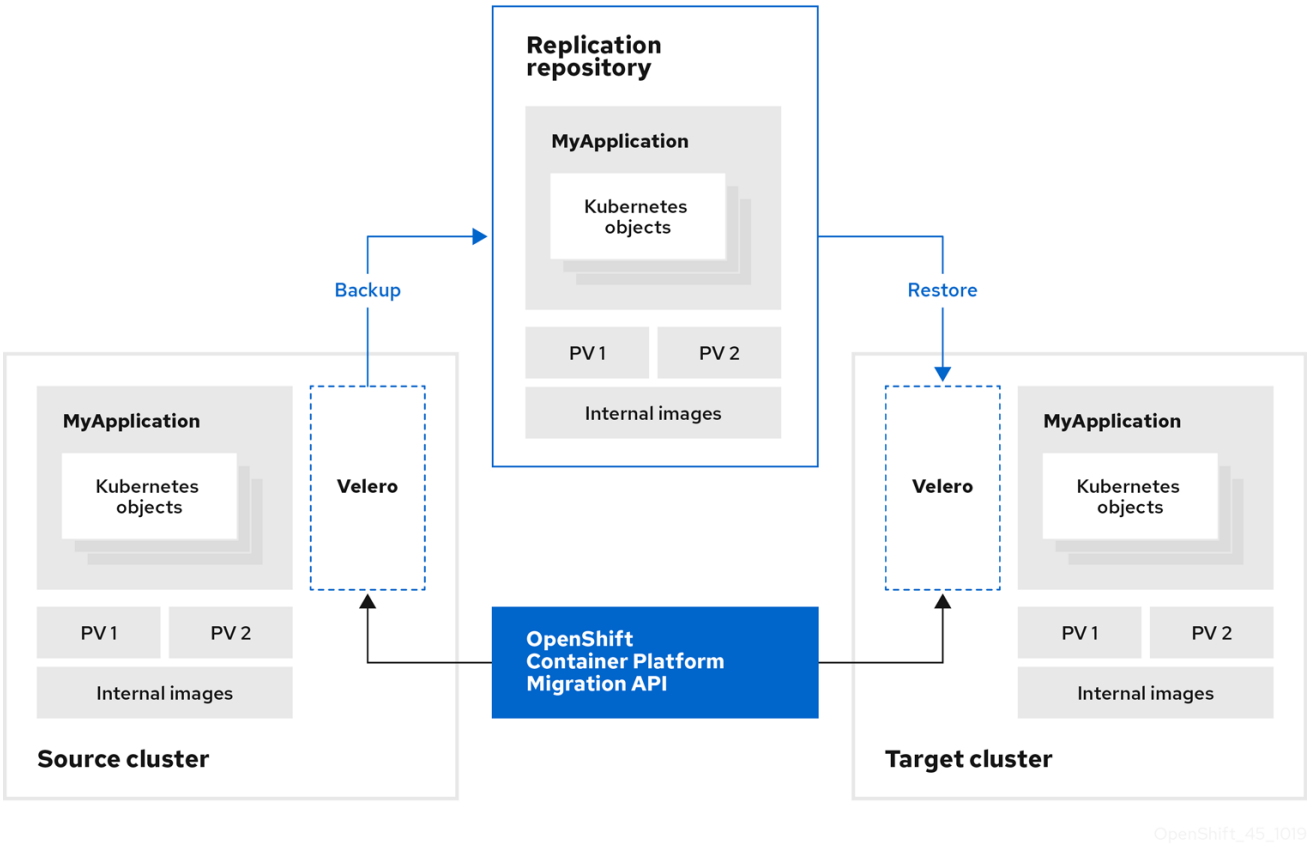
     虽然复制仓库没有出现在此图表中，但迁移需要它。



6. 运行迁移计划，使用以下选项之一：

   - **stage** 在不停止应用程序的情况下将数据复制到目标集群。
     阶段迁移可以多次运行，以便在迁移前将大多数数据复制到目标。运行一个或多个阶段迁移可缩短迁移的持续时间。

   - **cutover** 会停止源集群上的应用程序，并将资源移到目标集群。
     可选：您可以清除 **Halt transactions on the source cluster during migration**多选设置。



1.3. 关于数据复制方法

Migration Toolkit for Containers (MTC) 支持将数据从源集群迁移到目标集群的文件系统和快照数据复制方法。您可以选择适合于您的环境并受您的存储供应商支持的方法。

1.3.1. 文件系统复制方法

MTC 工具将数据文件从源集群复制到复制存储库，并从那里复制到目标集群。

文件系统复制方法使用 Restic 进行间接迁移，或使用 Rsync 进行直接卷迁移。

表 1.2. 文件系统复制方法概述

优点	限制
• 集群可以有不同的存储类。 • 所有 S3 存储供应商都支持。 • 使用 checksum 验证数据（可选）。 • 支持直接卷迁移，这会显著提高性能。	• 比快照复制方法慢。 • 可选的数据校验可能会显著降低性能。

注意

Restic 和 Rsync PV 迁移假设支持的 PV 仅是 **volumeMode=filesystem**。*不支持*在文件系统迁移中使用 **volumeMode=Block**。

1.3.2. 快照复制方法

MTC 将源集群数据的快照复制到云供应商的复制仓库。数据在目标集群上恢复。

快照复制方法可用于 Amazon Web Services、Google Cloud Provider 和 Microsoft Azure。

表 1.3. 快照复制方法概述

优点	限制
• 比文件系统复制方法快。	• 云供应商必须支持快照。 • 集群必须位于相同的云供应商。 • 集群必须位于同一位置或区域。 • 集群必须具有相同的存储类。 • 存储类必须与快照兼容。 • 不支持直接卷迁移。

1.4. 直接卷迁移和直接镜像迁移

您可以使用直接镜像迁移（DIM）和直接卷迁移（DVM）将镜像和数据直接从源集群迁移到目标集群。

如果您使用位于不同可用区的节点运行 DVM，迁移可能会失败，因为迁移的 pod 无法访问持久性卷声明。

DIM 和 DVM 具有显著的性能优势，因为跳过将文件从源集群备份到复制存储库以及从复制存储库恢复到目标集群的中间步骤。使用 Rsync 传输数据。

DIM 和 DVM 还有其他先决条件。

第 2 章 MTC 发行注记

2.1. MIGRATION TOOLKIT FOR CONTAINERS 1.8 发行注记

该版本的 Migration Toolkit for Containers 发行注记介绍了新的功能和增强功能、已弃用的功能以及已知的问题。

MTC（Migration Toolkit for Containers）可让您按照命名空间将应用程序工作负载在不同 OpenShift Container Platform 集群间进行迁移。

您可以从 OpenShift Container Platform 3 迁移到 4.15，也可以在 OpenShift Container Platform 4 集群之间迁移。

MTC 提供了一个基于 Kubernetes 自定义资源的 web 控制台和 API，可帮助您控制迁移并最小化应用程序停机时间。

有关 MTC 支持政策的信息，请参阅 OpenShift Application and Cluster Migration Solutions，它是 *Red Hat OpenShift Container Platform 生命周期政策*的一部分。

2.1.1. Migration Toolkit for Containers 1.8.3 发行注记

2.1.1.1. 技术变化

Migration Toolkit for Containers (MTC) 1.8.3 有以下技术变化：

现在支持 OADP 1.3

MTC 1.8.3 添加了对 OpenShift API for Data Protection (OADP) 的支持，作为 MTC 1.8.z 的依赖。

2.1.1.2. 已解决的问题

此发行版本有以下主要解决的问题：

CVE-2024-24786: Golang protobuf 模块中的一个错误会导致 unmarshal 函数进入死循环

在以前的 MTC 版本中，在 Golang 的 **protobuf** 模块中发现了一个漏洞，在处理某些无效输入时，**unmarshal** 函数会进入一个死循环。因此，攻击者可以利用这个漏洞，通过一个精心构建的无效输入，会导致这个函数进入死循环。

在这个版本中，**unmarshal** 功能可以正常工作。

如需更多信息，请参阅 CVE-2024-24786。

CVE-2023-45857: Axios Cross-Site Request Forgery 安全漏洞

在以前的 MTC 版本中，在 Axios 1.5.1 中发现了一个漏洞，它会被利用来发现存储在 Cookie 中的敏感的 **XSRF-TOKEN**，方法是在向主机发出的每个请求的 HTTP 标头 **X-XSRF-TOKEN** 中包括它。

如需更多信息，请参阅 CVE-2023-45857。

当源工作负载没有静止时，Restic 备份无法正常工作

在以前的 MTC 版本中，当使用路由部署应用程序时，一些文件不会被迁移。当源工作负载取消选择 quiesce 选项时，Restic 备份无法正常工作。

这个问题已在 MTC 1.8.3 中解决。

如需更多信息，请参阅 BZ#2242064。

因为 Velero 中的一个不被支持的值错误，Migration Controller 无法安装

因为 Velero 不支持的值错误，**MigrationController** 无法安装。将 OADP 1.3.0 更新至 OADP 1.3.1 可解决这个问题。如需更多信息，请参阅 BZ#2267018。

这个问题已在 MTC 1.8.3 中解决。

有关所有已解决的问题的完整列表，请参阅 JIRA 中的 MTC 1.8.3 解决的问题 列表。

2.1.1.3. 已知问题

MTC 有以下已知问题：

在 OpenShift Container Platform 4.12 中无法迁移服务帐户关联的 SCC

OpenShift Container Platform 版本 4.12 中服务帐户的相关安全性上下文约束 (SCC) 无法迁移。计划在以后的 MTC 版本中解决这个问题。(MIG-1454)

有关所有已知问题的完整列表，请参阅 JIRA 中的 MTC 1.8.3 已知问题列表。

2.1.2. Migration Toolkit for Containers 1.8.2 发行注记

2.1.2.1. 已解决的问题

此发行版本有以下主要解决的问题：

在设置自定义 CA 复制存储库后备份阶段失败

在以前的 MTC 版本中，在编辑复制存储库后，添加自定义 CA 证书、成功连接仓库并触发迁移，在备份阶段出现问题。

CVE-2023-26136: 在 4.1.3 之前使用 tough-cookie 软件包会受到 Prototype Pollution 的攻击

在以前的 (MTC) 版本中，MTC 中使用的 **tough-cookie** 软件包版本 4.1.3 会被受到原型处理的影响。发生此漏洞的原因是，当 **rejectPublicSuffixes** 的值设置为 **false** 时，CookieJar 无法正确处理 Cookie。

如需了解更多详细信息，请参阅 (CVE-2023-26136)

CVE-2022-25883 openshift-migration-ui-container: nodejs-semver: Regular expression 拒绝服务

在以前的(MTC)版本中，当不受信任的用户数据作为 **newRange** 提供时，MTC 中使用的 7.5.2 之前的 **semver** 软件包版本容易受到 Regular Expression Denial 的 Service (ReDoS)的攻击。

如需了解更多详细信息，请参阅 (CVE-2022-25883)

2.1.2.2. 已知问题

这个版本没有主要已知的问题。

2.1.3. Migration Toolkit for Containers 1.8.1 发行注记

2.1.3.1. 已解决的问题

此发行版本有以下主要解决的问题：

CVE-2023-39325: golang: net/http, x/net/http2: 快速流重置可能会导致过量工作

在处理 HTTP/2 协议（被 MTC 使用）中的多路流中发现了一个安全漏洞。 客户端可以重复请求新的多路流，并立即发送 **RST_STREAM** 帧来取消它。这在设置和分离流方面为服务器创建额外的工作负载，同时避免每个连接的最大活跃流数量的服务器端限制，从而导致因为服务器资源消耗而拒绝服务。(BZ#2245079)

建议升级到 MTC 1.8.1 或更高版本，从而解决了这个问题。

如需了解更多详细信息，请参阅 (CVE-2023-39325) 和 (CVE-2023-44487)

2.1.3.2. 已知问题

这个版本没有主要已知的问题。

2.1.4. Migration Toolkit for Containers 1.8.0 发行注记

2.1.4.1. 已解决的问题

此发行版本有以下解决的问题：

间接迁移会一直处于备份阶段

在以前的版本中，由于 **InvalidImageName** 错误，间接迁移会一直处于备份阶段。(BZ#2233097)

PodVolumeRestore 会保留在 In Progress 状态，使迁移一直处于 Stage Restore 状态

在以前的版本中，在执行间接迁移时，迁移会停留在 **Stage Restore** 步骤中，等待 **podvolumerestore** 完成。(BZ#2233868)

迁移的应用程序无法从目标集群上的内部 registry 中拉取镜像

在以前的版本中，在将应用程序迁移到目标集群时，迁移的应用程序无法从内部镜像 registry 中拉取镜像，从而导致 **应用程序失败**。(BZ#2233103)

由于授权问题，在 Azure 上迁移失败

在以前的版本中，在 Azure 集群中，当备份到 Azure 存储时，迁移会在 **Backup** 阶段失败。(BZ#2238974)

2.1.4.2. 已知问题

这个版本有以下已知问题：

升级 MTC 1.7.x → 1.8.x 时不会删除旧的 Restic pod

在这个发行版本中，当将 MTC Operator 从 1.7.x 升级到 1.8.x 时，旧的 Restic pod 不会被删除。因此，在升级后，Restic 和 node-agent pod 仍然可以在命名空间中看见。(BZ#2236829)

迁移的构建器 pod 无法推送到镜像 registry

在本发行版本中，在将包含 **BuildConfig** 的应用程序从源迁移到目标集群时，builder pod 会导致 **错误**，无法将镜像推送到镜像 registry。(BZ#2234781)

[UI] CA 捆绑包文件字段没有被正确清除

在本发行版本中，在启用 **Require SSL 验证** 并将内容添加到 MigStorage 的 MCG NooBaa 存储桶的 CA 捆绑包文件中后，连接会如预期失败。但是，通过删除 CA 捆绑包内容并清除 **Require SSL 验证** 来恢复这些更改时，连接仍会失败。该问题仅通过删除和重新添加存储库来解决。(BZ#2240052)

在设置自定义 CA 复制存储库后备份阶段失败

在(MTC)编辑复制存储库后，添加自定义 CA 证书、成功连接仓库并触发迁移，在备份阶段出现问题。

这个问题已在 MTC 1.8.2 中解决。

CVE-2023-26136: 在 4.1.3 之前使用 tough-cookie 软件包会受到 Prototype Pollution 的攻击

MTC 中使用的 4.1.3 **tough-cookie** 软件包版本之前（在 MTC 中使用）容易受到对轮询建模的攻击。此漏洞发生，因为当 **rejectPublicSuffixes** 的值设置为 **false** 时，CookieJar 无法正确处理 Cookie。

这个问题已在 MTC 1.8.2 中解决。

如需了解更多详细信息，请参阅 (CVE-2023-26136)

CVE-2022-25883 openshift-migration-ui-container: nodejs-semver: Regular expression 拒绝服务

在以前的(MTC)版本中，当不受信任的用户数据作为 **newRange** 提供时，MTC 中使用的 7.5.2 之前的 **semver** 软件包版本容易受到 Regular Expression Denial 的 Service (ReDoS)的攻击。

这个问题已在 MTC 1.8.2 中解决。

如需了解更多详细信息，请参阅 (CVE-2022-25883)

2.1.4.3. 技术变化

此发行版本有以下技术更改：

- 从 OpenShift Container Platform 3 迁移到 OpenShift Container Platform 4 需要旧的 MTC Operator 和 MTC 1.7.x。
- 不支持从 MTC 1.7.x 迁移到 MTC 1.8.x。
- 您必须使用 MTC 1.7.x 来迁移使用 OpenShift Container Platform 4.9 或更早版本源的任何内容。
  - MTC 1.7.x 必须在源和目标中使用。
- MTC 1.8.x 仅支持从 OpenShift Container Platform 4.10 或更高版本迁移到 OpenShift Container Platform 4.10 或更高版本。对于仅涉及集群版本 4.10 或更高版本的迁移，可以使用 1.7.x 或 1.8.x。但是，在源和目标上 MTC 1.Y.z 必须相同。
  - 不支持从源 MTC 1.7.x 迁移到目标 MTC 1.8.x。
  - 不支持从源 MTC 1.8.x 迁移到目标 MTC 1.7.x。
  - 支持从源 MTC 1.7.x 迁移到目标 MTC 1.7.x。
  - 支持从源 MTC 1.8.x 迁移到目标 MTC 1.8.x。
- MTC 1.8.x 默认会安装 OADP 1.2.x。
- 从 MTC 1.7.x 升级到 MTC 1.8.0，需要手动将 OADP 频道改为 1.2。如果没有这样做，Operator 升级会失败。

2.2. MIGRATION TOOLKIT FOR CONTAINERS 1.7 发行注记

该版本的 Migration Toolkit for Containers 发行注记介绍了新的功能和增强功能、已弃用的功能以及已知的问题。

MTC（Migration Toolkit for Containers）可让您按照命名空间将应用程序工作负载在不同 OpenShift Container Platform 集群间进行迁移。

您可以从 OpenShift Container Platform 3 迁移到 4.15，也可以在 OpenShift Container Platform 4 集群之间迁移。

MTC 提供了一个基于 Kubernetes 自定义资源的 web 控制台和 API，可帮助您控制迁移并最小化应用程序停机时间。

有关 MTC 支持政策的信息，请参阅 OpenShift Application and Cluster Migration Solutions，它是 *Red Hat OpenShift Container Platform 生命周期政策*的一部分。

2.2.1. Migration Toolkit for Containers 1.7.16 发行注记

2.2.1.1. 已解决的问题

此发行版本有以下解决的问题：

CVE-2023-45290: Golang: net/http: Memory exhaustion in the Request.ParseMultipartForm method

net/http Golang 标准库软件包中发现了一个安全漏洞，它会影响 MTC 的早期版本。在以前的版本中，当解析 **multipart** 表单时，可以明确使用 **Request.ParseMultipartForm**，或使用 **Request.FormValue**, **Request.PostFormValue**, 或 **Request.FormFile** 方法隐式应用，解析表单的总大小限制不适用于在读单一表单行时消耗的内存。这可能会允许在恶意设计的输入中包含非常长的行，从而导致分配大量内存，这可能会导致内存耗尽。

要解决这个问题，升级到 MTC 1.7.16。

如需了解更多详细信息，请参阅 CVE-2023-45290

CVE-2024-24783: Golang: crypto/x509: Verify panics on certificates with an unknown public key algorithm

在 **crypto/x509** Golang 标准库软件包中发现了一个安全漏洞，它会影响 MTC 的早期版本。验证包含带有未知公钥算法的证书的证书链会导致 **Certificate.Verify** panic。这会影响将 **Config.ClientAuth** 设置为 **VerifyClientCertIfGiven** 或 **RequireAndVerifyClientCert** 的所有 **crypto/tls** 客户端和服务器。默认行为是 TLS 服务器无法验证客户端证书。

要解决这个问题，升级到 MTC 1.7.16。

如需了解更多详细信息，请参阅 CVE-2024-24783。

CVE-2024-24784: Golang: net/mail: 显示名称中的注释被错误处理

net/mail Golang 标准库软件包中发现了一个安全漏洞，它会影响 MTC 的早期版本。 **ParseAddressList** 函数错误地处理注释、文本（括号中的文本）和显示名称。由于这与地址解析程序不匹配，因此可能会导致使用不同解析器的程序进行不同的信任决策。

要解决这个问题，升级到 MTC 1.7.16。

如需了解更多详细信息，请参阅 CVE-2024-24784。

CVE-2024-24785: Golang: html/template: Errors returned from MarshalJSON methods may break template escaping

在 **html/template** Golang 标准库软件包中发现了一个安全漏洞，它会影响 MTC 的早期版本。 如果来自 **MarshalJSON** 方法返回的错误包含用户控制的数据，则它们可能会用来破坏 **html/template** 软件包的上下文自动转义行为，以便后续操作将意外内容注入模板。

要解决这个问题，升级到 MTC 1.7.16。

如需了解更多详细信息，请参阅 CVE-2024-24785。

CVE-2024-29180: webpack-dev-middleware: Lack of URL validation may lead to file leak

webpack-dev-middleware 软件包 中发现了一个安全漏洞，它会影响 MTC 的早期版本。在返回本地文件前，这个缺陷无法验证提供的 URL 地址，这可让攻击者编写 URL 来从开发人员机器返回任意本地文件。

要解决这个问题，升级到 MTC 1.7.16。

如需了解更多详细信息，请参阅 CVE-2024-29180。

CVE-2024-30255: envoy: HTTP/2 CPU exhaustion due to CONTINUATION frame flood

在 **envoy** 代理如何实现 HTTP/2 codec 中发现了一个安全漏洞，这会影响早期版本的 MTC。对可在单一流内发送的 **CONTINUATION** 帧数量有不足的限制，即使超过 **envoy** 的标题映射限制。这个漏洞可能会允许未经身份验证的远程攻击者向存在安全漏洞的服务器发送数据包。这些数据包可能会消耗计算资源并导致拒绝服务(DoS)。

要解决这个问题，升级到 MTC 1.7.16。

如需了解更多详细信息，请参阅 CVE-2024-30255。

2.2.1.2. 已知问题

这个版本有以下已知问题：

直接卷迁移失败，因为源集群中的 Rsync pod 进入 Error 状态

在使用持久性卷声明(PVC)迁移任何应用程序时，**Stage** migration 操作会成功显示警告，而直接卷迁移(DVM)会失败，源命名空间中的 **rsync** pod 会进入 **error** 状态。(BZ#2256141)

冲突条件会在创建后被清除

在创建导致冲突错误消息的新状态迁移计划时，错误消息会在显示后很快清除。(BZ#2144299)

当集群中配置了不同提供程序类型的多个卷快照位置时，迁移会失败

当具有不同供应商类型的集群中有多个卷快照位置(VSL)时，但没有将任何它们设置为默认的 VSL，Velero 会导致迁移操作失败。(BZ#2180565)

2.2.2. Migration Toolkit for Containers 1.7.15 发行注记

2.2.2.1. 已解决的问题

此发行版本有以下解决的问题：

CVE-2024-24786: 在 Golang 的 protobuf 模块中发现了一个安全漏洞，unmarshal 功能可以进入一个死循环

在 **protojson.Unmarshal** 函数中发现了一个安全漏洞，它可能会导致函数在 unmarshaling 特定的无效 JSON 消息时进入死循环。当 unmarshaling 到一个包括了 **google.protobuf.Any** 值的信息或在 JSON 格式的消息中设置了 **UnmarshalOptions.DiscardUnknown** 选项时，这个条件会发生。

要解决这个问题，升级到 MTC 1.7.15。

如需了解更多详细信息，请参阅 (CVE-2024-24786)。

CVE-2024-28180: jose-go 错误处理高度压缩的数据

在 Jose 中发现了一个因为处理高压缩数据不当造成的漏洞。攻击者可以发送一个 JSON Web 加密(JWE)加密消息，其中包含在解压缩 **Decrypt** 或 **DecryptMulti** 功能时使用的大量内存和 CPU 的压缩数据。

要解决这个问题，升级到 MTC 1.7.15。

如需了解更多详细信息，请参阅 (CVE-2024-28180)。

2.2.2.2. 已知问题

这个版本有以下已知问题：

直接卷迁移失败，因为源集群中的 Rsync pod 进入 Error 状态

在使用持久性卷声明(PVC)迁移任何应用程序时，**Stage** migration 操作会成功显示警告，而直接卷迁移(DVM)会失败，源命名空间中的 **rsync** pod 会进入 **error** 状态。(BZ#2256141)

冲突条件会在创建后被清除

在创建导致冲突错误消息的新状态迁移计划时，错误消息会在显示后很快清除。(BZ#2144299)

当集群中配置了多个不同提供程序类型的卷快照位置(VSL)时，迁移会失败，且没有指定默认 VSL。

当集群中具有不同提供程序类型的集群中有多个 VSL，并且没有设置它们作为默认的 VSL，Velero 会产生一个验证错误，导致迁移操作失败。(BZ#2180565)

2.2.3. Migration Toolkit for Containers 1.7.14 发行注记

2.2.3.1. 已解决的问题

此发行版本有以下解决的问题：

CVE-2023-39325 CVE-2023-44487: 各种安全漏洞

在处理 HTTP/2 协议（被 MTC 使用）中的多路流中发现了一个安全漏洞。 客户端可以重复请求新的多路流，然后立即发送 **RST_STREAM** 帧来取消这些请求。对于设置和分离流，这个活动会为服务器创建额外的工作负载，但避免了每个连接的最大活跃流数量的服务器端限制。这会导致因为服务器的资源被耗尽而出现拒绝服务的问题。

- (BZ#2243564)
- (BZ#2244013)
- (BZ#2244014)

- (BZ#2244015)
- (BZ#2244016)
- (BZ#2244017)

要解决这个问题，升级到 MTC 1.7.14。

如需了解更多详细信息，请参阅 (CVE-2023-44487) 和 (CVE-2023-39325)。

CVE-2023-39318 CVE-2023-39319 CVE-2023-39321: 各种安全漏洞

- (CVE-2023-39318): 在 Golang 中发现了一个安全漏洞，它被 MTC 使用。 **html/template** 软件包没有正确处理类似 HTML 的 **""** 注释令牌，或者在 **<script>** 上下文中正确处理 hashbang **"#!"** 注释令牌。此漏洞可能会导致模板解析器错误地解释 **<script>** 上下文的内容，从而导致操作被不当转义。
  - (BZ#2238062)
  - (BZ#2238088)
- (CVE-2023-39319): 在 Golang 中发现了一个安全漏洞，它被 MTC 使用。对于 <script> 中的 JavaScript 代码， **html/template** 软件包没有应用正确的规则来处理同时存在的 **"<script"**, **"<!--"**, 和 **"</script"**。这可能会导致模板解析器错误地认为脚本已结束，从而导致操作被不当转义。
  - (BZ#2238062)
  - (BZ#2238088)
- (CVE-2023-39321): 在 Golang 中发现了一个安全漏洞，它被 MTC 使用。为 QUIC 连接处理不完整的 post-handshake 消息可能会导致 panic。
  - (BZ#2238062)
  - (BZ#2238088)
- (CVE-2023-3932): 在 Golang 中发现了一个安全漏洞，它被 MTC 使用。使用 QUIC 传输协议进行连接时，当在读取握手后消息时对缓冲区的数据量没有设置上限，从而使恶意的 QUIC 连接可以导致内存的使用大量增加。
  - (BZ#2238088)

要解决这个问题，升级到 MTC 1.7.14。

如需了解更多详细信息，请参阅 (CVE-2023-39318), (CVE-2023-39319) 和 (CVE-2023-39321)。

2.2.3.2. 已知问题

这个版本没有主要已知的问题。

2.2.4. Migration Toolkit for Containers 1.7.13 发行注记

2.2.4.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.4.2. 已知问题

这个版本没有主要已知的问题。

2.2.5. Migration Toolkit for Containers 1.7.12 发行注记

2.2.5.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.5.2. 已知问题

这个版本有以下已知问题：

Migration details 页面中会显示错误代码 504

在 Migration details 页面中，首先会显示 **迁移详情**，且没有任何问题。但是，在一段时间后，详情会消失，并返回 **504** 错误。(BZ#2231106)

将 MTC 1.7.x 升级到 MTC 1.8 时不会删除旧的 restic pod

在将 MTC operator 从 1.7.x 升级到 1.8.x 时，旧的 restic pod 不会被删除。升级后，restic 和 node-agent pod 在命名空间中可见。(BZ#2236829)

2.2.6. Migration Toolkit for Containers 1.7.11 发行注记

2.2.6.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.6.2. 已知问题

这个版本没有已知的问题。

2.2.7. Migration Toolkit for Containers 1.7.10 发行注记

2.2.7.1. 已解决的问题

此发行版本包括以下已解决的问题：

调整 DVM 中的 rsync 选项

在这个发行版本中，您可以防止在直接卷迁移 (DVM) 过程中使用 Rsync 对绝对符号链接进行操作。以特权模式运行 DVM 会在持久性卷声明 (PVC) 内保留绝对符号链接。要切换到特权模式，在 **MigrationController** CR 中，将 **migration_rsync_privileged** spec 设置为 **true**。(BZ#2204461)

2.2.7.2. 已知问题

这个版本没有已知的问题。

2.2.8. Migration Toolkit for Containers 1.7.9 发行注记

2.2.8.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.8.2. 已知问题

此发行版本有以下已知问题：

调整 DVM 中的 rsync 选项

在这个发行版本中，用户无法防止在直接卷迁移(DVM)期间通过 rsync 操作绝对符号链接。(BZ#2204461)

2.2.9. Migration Toolkit for Containers 1.7.8 发行注记

2.2.9.1. 已解决的问题

此发行版本有以下主要解决的问题：

在 MTC operator 中无法覆盖 Velero 镜像

在以前的版本中，无法使用 **MigrationController** 自定义资源(CR)中的 **velero_image_fqin** 参数覆盖 velero 镜像。(BZ#2143389)

当域名有超过 6 个字符时，从 UI 添加一个 MigCluster 会失败

在以前的版本中，当域名有超过 6 个字符时，从 UI 添加一个 MigCluster 会失败。UI 代码预期有两个到六个字符之间的域名。(BZ#2152149)

UI 无法呈现 Migrations' 页面： Cannot read properties of undefined (reading 'name')

在以前的版本中，UI 无法呈现 Migrations' 页面，返回 **Cannot read properties of undefined (reading 'name')**。(BZ#2163485)

在 Red Hat OpenShift Container Platform 4.6 集群中创建 DPA 资源失败

在以前的版本中，当在 OpenShift Container Platform 4.6 集群上部署 MTC 时，根据日志创建 DPA 会失败，这会导致一些 pod 缺少。从 OCP 4.6 集群中的 migration-controller 中的日志，它表示传递了意外的 **null** 值，这会导致错误。(BZ#2173742)

2.2.9.2. 已知问题

这个版本没有已知的问题。

2.2.10. Migration Toolkit for Containers 1.7.7 发行注记

2.2.10.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.10.2. 已知问题

这个版本没有已知的问题。

2.2.11. Migration Toolkit for Containers 1.7.6 发行注记

2.2.11.1. 新功能

在 Red Hat OpenShift Container Platform 4.12 中使用 PSA 实现 DVM 支持的建议更改

随着 OpenShift Container Platform 4.12 中的 Pod Security Admission (PSA)的传入强制，默认 pod 会使用 **restricted** 配置集运行。这个 **restricted** 配置集意味着要迁移的工作负载将违反此策略，且现在不再可以正常工作。以下功能增强概述了与 OCP 4.12 兼容所需的更改。(MIG-1240)

2.2.11.2. 已解决的问题

此发行版本有以下主要解决的问题：

由于 Red Hat OpenShift Platform 4.12 中缺少 cronjob 错误，则无法创建存储类 Conversion 计划

在以前的版本中，在持久性卷页面中，抛出一个错误，即 CronJob 在版本 **batch/v1beta1** 中不可用，并在点 cancel 时创建 migplan，其状态为 **Not ready**。(BZ#2143628)

2.2.11.3. 已知问题

此发行版本有以下已知问题：

冲突条件会在创建后被清除

在创建会导致冲突错误的新状态迁移计划时，这个错误会在显示后被清除。(BZ#2144299)

2.2.12. Migration Toolkit for Containers 1.7.5 发行注记

2.2.12.1. 已解决的问题

此发行版本包括以下已解决的问题：

直接卷迁移作为源集群上的 rsync pod 失败，进入 Error 状态

在以前的版本中，迁移成功并显示警告，但使用源命名空间中的 rsync pod 进入错误状态的直接卷迁移失败。(*BZ#2132978)

2.2.12.2. 已知问题

这个版本有以下已知问题：

在 MTC operator 中无法覆盖 Velero 镜像

在以前的版本中，无法使用 **MigrationController** 自定义资源(CR)中的 **velero_image_fqin** 参数覆盖 velero 镜像。(BZ#2143389)

在 UI 中编辑 MigHook 时，页面可能无法重新加载

如果出现网络连接问题，则 UI 在编辑 hook 时可能无法重新加载。恢复网络连接后，页面将无法重新加载，直到缓存被清除为止。(BZ#2140208)

2.2.13. Migration Toolkit for Containers 1.7.4 发行注记

2.2.13.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.13.2. 已知问题

回滚没有从目标集群中删除某些资源

在从 MTC UI 执行应用程序回滚时，一些资源不会从目标集群中删除，回滚会显示成功的状态。(BZ#2126880)

2.2.14. Migration Toolkit for Containers 1.7.3 发行注记

2.2.14.1. 已解决的问题

此发行版本有以下主要解决的问题：

目标命名空间的正确 DNS 验证

在以前的版本中，如果目标命名空间使用非字母字符启动，则 MigPlan 无法验证。(BZ#2102231)

从 UI 取消选择所有 PVC 仍然会导致尝试的 PVC 传输

在以前的版本中，在进行完整迁移时，取消选择持久性卷声明(PVC)不会跳过选择 PVC，并仍然尝试迁移它们。(BZ#2106073)

目标命名空间的 DNS 验证不正确

在以前的版本中，MigPlan 无法验证，因为目标命名空间使用非字母字符启动。(BZ#2102231)

2.2.14.2. 已知问题

这个版本没有已知的问题。

2.2.15. Migration Toolkit for Containers 1.7.2 发行注记

2.2.15.1. 已解决的问题

此发行版本有以下主要解决的问题：

MTC UI 无法正确显示日志

在以前的版本中，MTC UI 无法正确显示日志。(BZ#2062266)

StorageClass 转换计划在 migplan 中添加 migstorage 参考

在以前的版本中，StorageClass 转换计划有一个 **migstorage** 引用，即使还没有使用它。(BZ#2078459)

下载的日志中缺少 Velero pod 日志

在以前的版本中，当为所有日志下载压缩(.zip)文件夹时，会缺少 velero pod。(BZ#2076599)

UI 下拉菜单中缺少 Velero pod 日志

在以前的版本中，在执行迁移后，velero pod 日志没有包含在下拉列表中提供的日志中。(BZ#2076593)

rsync 选项日志无法在 log-reader pod 中看到

在以前的版本中，当试图在 **migrationcontroller** 中设置任何有效或无效的 rsync 选项时，log-reader 不会显示有关无效选项或正在使用的 rsync 命令的任何日志。(BZ#2079252)

Velero/Restic 上的默认 CPU 请求过于要求，在某些情况下会失败

在以前的版本中，Velero/Restic 上的默认 CPU 请求过于要求并在某些环境中失败。Velero 和 Restic Pod 的默认 CPU 请求被设置为 500m。这些值非常高。(BZ#2088022)

2.2.15.2. 已知问题

这个版本有以下已知问题：

UI 不遵守将复制存储库更新到不同的存储供应商类型

将复制存储库更新为不同的类型并点 **Update Repository** 后，它会显示连接成功，但不会使用正确的详情更新 UI。当再次点 **Edit** 按钮时，它仍然会显示旧的复制存储库信息。

另外，当尝试再次更新复制存储库时，它仍然会显示旧的复制详情。在选择新存储库时，它还会显示您之前输入的所有信息，并且没有启用 **Update repository**，因为没有提交更改。(BZ#2102020)

迁移失败，因为没有找到备份

因为没有找到初始备份，迁移在恢复阶段失败。(BZ#2104874)

更新 Azure 资源组时不会启用更新 Cluster 按钮

在更新远程集群时，选择 **Azure 资源组** 复选框，添加资源组不会启用 **Update cluster** 选项。(BZ#2098594)

删除 migstorage 资源的 UI 中的弹出错误

在 OpenShift Container Platform 中创建 **backupStorage** 凭证 secret 时，如果从 UI 中删除 **migstorage**，则返回 404 错误，且不会删除底层 secret。(BZ#2100828)

MigAnalytic 资源在 UI 中显示资源数为 0

从后端创建 migplan 后，Miganalytic 资源会在 UI 中显示为 **0**。(BZ#2102139)

当将两个尾部斜杠添加到公开路由主机到镜像 registry 时，registry 验证会失败

在向公开的 registry 路由中添加两个尾部斜杠（即 // ）后，MigCluster 资源会显示为 **已连接** 的状态。当使用 DIM 从后端创建 migplan 时，计划将移至 **未就绪** 状态。(BZ#2104864)

在编辑源集群时，Service Account Token 不可见

在编辑添加并处于 **Connected** 状态的源集群时，在 UI 中无法看到服务帐户令牌。要保存向导，您必须再次获取令牌，并在字段内提供详情。(BZ#2097668)

2.2.16. Migration Toolkit for Containers 1.7.1 发行注记

2.2.16.1. 已解决的问题

这个版本没有主要解决的问题。

2.2.16.2. 已知问题

这个版本有以下已知问题：

目标命名空间的 DNS 验证不正确

PlanPlan 无法被验证，因为目标命名空间以非字母字符开头。(BZ#2102231)

因为 Velero pod 中缺少标签，迁移控制器中的云传播阶段无法正常工作

因为 Velero pod 中缺少标签，迁移控制器中的 Cloud propagation 阶段无法正常工作。迁移控制器中的 **EnsureCloudSecretPropagated** 阶段会等待两个端传播复制存储库 secret。因为 Velero pod 缺少该标签，所以该阶段无法正常工作。(BZ#2088026)

在某些环境中进行调度失败时，Velero/Restic 上的默认 CPU 请求过于要求

在某些环境中进行调度失败时，Velero/Restic 上的默认 CPU 请求过于要求。Velero 和 Restic Pod 的默认 CPU 请求被设置为 500m。这些值非常高。可以使用 Velero 和 Restic 的 **podConfig** 字段在 DPA 中配置资源。迁移 Operator 应该将 CPU 请求设置为较低值，如 100m，以便 Velero 和 Restic pod 可以在资源受限环境中调度，这通常运行。(BZ#2088022)

编辑存储类转换计划后，PersistentVolumeVolumes 页面中会显示警告

编辑存储类转换计划后，**persistentVolumes** 页面中会显示警告信息。在编辑现有迁移计划时，在 UI 上会显示一个警告，**At least one PVC must be selected for Storage Class Conversion**。(BZ#2079549)

下载的日志中缺少 Velero pod 日志

当为所有日志下载压缩(.zip)文件夹时，velero pod 缺失。(BZ#2076599)

UI 下拉菜单中缺少 Velero pod 日志

执行迁移后，velero pod 日志不会包含在下拉列表中提供的日志中。(BZ#2076593)

2.2.17. Migration Toolkit for Containers 1.7.0 发行注记

2.2.17.1. 新功能及功能增强

此发行版本有以下新功能和增强：

- Migration Toolkit for Containers(MTC)Operator 现在依赖于 OpenShift API for Data Protection(OADP)Operator。安装 MTC Operator 时，Operator Lifecycle Manager(OLM)会自动在同一命名空间中安装 OADP Operator。
- 您可以使用 **crane tunnel-api** 命令在两个集群间建立网络隧道，从位于防火墙后的源集群迁移到基于云的目标集群。
- 在 MTC web 控制台中转换存储类：您可以通过在同一集群中迁移持久性卷(PV)的存储类来转换它。

2.2.17.2. 已知问题

这个版本有以下已知问题：

- 当 AWS gp2 PVC 没有可用空间时，**MigPlan** 自定义资源不会显示警告。(BZ#1963927)
- 如果目标存储是由 AWS Elastic 文件系统(EFS)动态置备的 PV，则直接和间接数据传输无法正常工作。这是因为 AWS EFS Container Storage Interface(CSI)驱动程序的限制。(BZ#2085097)
- IBM Cloud 的块存储必须位于同一可用区中。请参阅针对虚拟私有云块存储的 IBM 常见问题解答。
- MTC 1.7.6 无法将支持 **v1beta1** cron 作业的源集群迁移到 OpenShift Container Platform 4.12 及更新的版本，不支持 **v1beta1** cron 作业。(BZ#2149119)

2.3. 容器迁移工具 1.6 发行注记

该版本的 Migration Toolkit for Containers 发行注记介绍了新的功能和增强功能、已弃用的功能以及已知的问题。

MTC（Migration Toolkit for Containers）可让您按照命名空间将应用程序工作负载在不同 OpenShift Container Platform 集群间进行迁移。

您可以从 OpenShift Container Platform 3 迁移到 4.15，也可以在 OpenShift Container Platform 4 集群之间迁移。

MTC 提供了一个基于 Kubernetes 自定义资源的 web 控制台和 API，可帮助您控制迁移并最小化应用程序停机时间。

有关 MTC 支持政策的信息，请参阅 OpenShift Application and Cluster Migration Solutions，它是 *Red Hat OpenShift Container Platform 生命周期政策*的一部分。

2.3.1. 容器迁移工具 1.6 发行注记

2.3.1.1. 新功能及功能增强

此发行版本有以下新功能和增强：

- 状态迁移：您可以选择特定的持久性卷声明 (PVC) 来执行可重复的、仅限状态的迁移。
- "new operator version available"通知：MTC web 控制台的 Clusters 页面在有新的 MTC Operator 可用时显示通知。

2.3.1.2. 已弃用的功能

以下功能已弃用：

- MTC 版本 1.4 不再被支持。

2.3.1.3. 已知问题

这个版本有以下已知问题：

- 在 OpenShift Container Platform 3.10 中，**MigrationController** pod 重启用时过长。Bugzilla 报告包含临时解决方案。(BZ#1986796)
- 在从 IBM Cloud 上的典型 OpenShift Container Platform 源集群直接迁移卷时，**Stage** pod 会失败。IBM 块存储插件不允许将同一卷挂载到同一节点的多个 pod。因此，PVC 无法同时挂载到 Rsync pod 和应用程序 pod 上。要解决这个问题，请在迁移前停止应用程序 pod。(BZ#1887526)
- 当 AWS gp2 PVC 没有可用空间时，**MigPlan** 自定义资源不会显示警告。(BZ#1963927)
- IBM Cloud 的块存储必须位于同一可用区中。请参阅针对虚拟私有云块存储的 IBM 常见问题解答。

2.4. MIGRATION TOOLKIT FOR CONTAINERS 1.5 发行注记

该版本的 Migration Toolkit for Containers 发行注记介绍了新的功能和增强功能、已弃用的功能以及已知的问题。

MTC（Migration Toolkit for Containers）可让您按照命名空间将应用程序工作负载在不同 OpenShift Container Platform 集群间进行迁移。

您可以从 OpenShift Container Platform 3 迁移到 4.15，也可以在 OpenShift Container Platform 4 集群之间迁移。

MTC 提供了一个基于 Kubernetes 自定义资源的 web 控制台和 API，可帮助您控制迁移并最小化应用程序停机时间。

有关 MTC 支持政策的信息，请参阅 OpenShift Application and Cluster Migration Solutions，它是 *Red Hat OpenShift Container Platform 生命周期政策*的一部分。

2.4.1. Migration Toolkit for Containers 1.5 发行注记

2.4.1.1. 新功能及功能增强

此发行版本有以下新功能和增强：

- Web 控制台的 **Migration 详情**页面中的 **Migration 资源**树通过用于监控和调试迁移的其他资源、Kubernetes 事件和实时状态信息进行了增强。
- Web 控制台支持数百个迁移计划。
- 源命名空间可以在迁移计划中映射到不同的目标命名空间。在以前的版本中，源命名空间映射到名称相同的目标命名空间。
- 在迁移过程中，Web 控制台中会显示带有状态信息的 hook 阶段。
- 在直接卷迁移过程中，web 控制台中会显示 Rsync 重试尝试的数量。
- 可以为直接卷迁移启用持久性卷 (PV) 大小，以确保目标集群不会出现磁盘空间不足的问题。
- 触发 PV 重新定义大小的阈值可以配置。在以前的版本中，当磁盘用量超过 97% 时，PV 会重新定义大小。
- Velero 已更新至 1.6 版本，它提供了大量修复和增强。
- 可以启用缓存的 Kubernetes 客户端来提高性能。

2.4.1.2. 已弃用的功能

以下功能已弃用：

- MTC 版本 1.2 和 1.3 不再被支持。
- 更新已弃用 API 的步骤已从文档的故障排除部分中删除，因为 **oc convert** 命令已弃用。

2.4.1.3. 已知问题

这个版本有以下已知问题：

- 如果您创建超过 400 个迁移计划，则 Microsoft Azure 存储不可用。**MigStorage** 自定义资源显示以下消息：**The request is being throttled as the limit has been reached for operation type**。（BZ#1977226）

- 如果迁移失败，迁移计划不会为静默的 pod 保留自定义持久性卷 (PV) 设置。您必须手动回滚，删除迁移计划，并使用 PV 设置创建新的迁移计划。(BZ#1784899)

- 对于 AWS gp2 存储，PV 大小重新定义无法正常工作，除非 **pv_resizing_threshold** 为 42% 或更高。（BZ#1973148）

- 在以下情况下，PV 重新定义大小不适用于 OpenShift Container Platform 3.7 和 3.9 源集群：

  - 应用程序是在安装 MTC 后安装的。

  - 安装 MTC 后，应用程序 pod 会被重新调度到其他节点上。
    OpenShift Container Platform 3.7 和 3.9 不支持 Mount Propagation 功能，它允许 Velero 在 **Restic** pod 中自动挂载 PV。**MigAnalytic** 自定义资源 (CR) 无法从 **Restic** pod 收集 PV 数据，并将资源报告为 **0**。**MigPlan** CR 显示类似如下的状态：

    输**出示例**

    ```
    status:
      conditions:
      - category: Warn
        lastTransitionTime: 2021-07-15T04:11:44Z
        message: Failed gathering extended PV usage information for PVs [nginx-logs nginx-
    html], please see MigAnalytic openshift-migration/ocp-24706-basicvolmig-migplan-
    1626319591-szwd6 for details
        reason: FailedRunningDf
        status: "True"
        type: ExtendedPVAnalysisFailed
    ```

    要启用 PV 大小调整，您可以在源集群中手动重启 Restic daemonset，或者在与应用程序相同的节点上重启 **Restic** pod。如果没有重启 Restic，在没有调整 PV 的情况下运行直接卷迁移。（BZ#1982729）

2.4.1.4. 技术变化

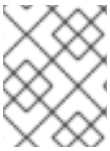
此发行版本有以下技术更改：

- 旧的 MTC Operator 版本 1.5.1 在 OpenShift Container Platform 版本 3.7 到 4.5 中手动安装。

- Migration Toolkit for Containers Operator 版本 1.5.1 在 OpenShift Container Platform 版本 4.6 及更新的版本中使用 Operator Lifecycle Manager 安装。

第 3 章 安装 MTC

您可以在 OpenShift Container Platform 4 上安装 MTC。



注意

要在 OpenShift Container Platform 3 上安装 MTC，请参阅在 OpenShift Container Platform 3 上安装旧的 MTC。

默认情况下，MTC web 控制台和 **Migration Controller** pod 在目标集群中运行。您可以配置 **Migration Controller** 自定义资源清单在远程集群中运行 MTC web 控制台和 **Migration Controller** pod。

安装 MTC 后，您必须配置对象存储以用作复制存储库。

要卸载 MTC，请参阅卸载 MTC 并删除资源。

3.1. 兼容性指南

您必须安装与 OpenShift Container Platform 版本兼容的 MTC。

定义

旧平台

OpenShift Container Platform 4.5 及更早版本。

现代平台

OpenShift Container Platform 4.6 及更新的版本。

旧 Operator

针对传统平台设计的 MTC Operator。

现代 operator

针对现代平台设计的 MTC Operator。

控制集群

运行 MTC 控制器和 GUI 的集群。

远程集群

运行 Velero 的迁移的源或目标集群。Control Cluster 通过 Velero API 与远程集群通信，以驱动迁移。

您必须使用兼容的 MTC 版本来迁移 OpenShift Container Platform 集群。要使迁移成功源集群和目标集群，必须使用相同的 MTC 版本。

MTC 1.7 支持从 OpenShift Container Platform 3.11 迁移到 4.9。

MTC 1.8 仅支持从 OpenShift Container Platform 4.10 及更新的版本进行迁移。

表 3.1. MTC 兼容性：从传统或现代平台迁移

详情	OpenShift Container Platform 3.11	OpenShift Container Platform 4.0 到 4.5	OpenShift Container Platform 4.6 到 4.9	OpenShift Container Platform 4.10 或更高版本
稳定 MTC 版本	MTC v.1.7.*z*	MTC v.1.7.*z*	MTC v.1.7.*z*	MTC v.1.8.*z*

详情	OpenShift Container Platform 3.11	OpenShift Container Platform 4.0 到 4.5	OpenShift Container Platform 4.6 到 4.9	OpenShift Container Platform 4.10 或更高版本
安装		旧版 MTC v.1.7.*z* operator：使用 **operator.yml** 文件手动安装。 [**重要信息**] 此集群不能是控制集群。	使用 OLM 安装，发行频道 **release-v1.7**	使用 OLM 安装，发行频道 **release-v1.8**

在某些情况下，网络的限制可能会阻止现代集群连接到迁移中需要涉及的其他集群。例如，当从内部的 OpenShift Container Platform 3.11 集群迁移到云环境中的现代 OpenShift Container Platform 集群时，，现代集群无法连接到 OpenShift Container Platform 3.11 集群。

在 MTC v.1.7.*z* 中，如果其中一个远程集群因为网络限制而无法与控制集群通信，请使用 **crane tunnel-api** 命令。

对于稳定（stable）的 MTC 发行版本，虽然您应该始终将最现代化的集群指定为控制集群，但是在这种情况下，可能需要将旧的集群指定为控制集群，并将工作负载推送到远程集群。

3.2. 在 OPENSHIFT CONTAINER PLATFORM 4.2 到 4.5 上安装旧的 MTC OPERATOR

您可以在 OpenShift Container Platform 版本 4.2 到 4.5 中手动安装旧的 MTC Operator。

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。
- 您必须有权访问 **registry.redhat.io**。
- 必须安装 **podman** 。

流程

1. 使用您的红帽客户门户网站账户登陆到 **registry.redhat.io**：

```
$ podman login registry.redhat.io
```

2. 输入以下命令下载 **operator.yml** 文件：

```
podman cp $(podman create registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-operator:v1.7):/operator.yml ./
```

3. 输入以下命令下载 **controller.yml** 文件：

```
podman cp $(podman create registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-operator:v1.7):/controller.yml ./
```

4. 登录您的 OpenShift Container Platform 源集群。
5. 验证集群可以在 **registry.redhat.io** 中进行身份验证：

```
$ oc run test --image registry.redhat.io/ubi9 --command sleep infinity
```

6. 创建 MTC Operator 对象的 Migration Toolkit:

```
$ oc create -f operator.yml
```

输**出示例**

```
namespace/openshift-migration created
rolebinding.rbac.authorization.k8s.io/system:deployers created
serviceaccount/migration-operator created
customresourcedefinition.apiextensions.k8s.io/migrationcontrollers.migration.openshift.io created
role.rbac.authorization.k8s.io/migration-operator created
rolebinding.rbac.authorization.k8s.io/migration-operator created
clusterrolebinding.rbac.authorization.k8s.io/migration-operator created
deployment.apps/migration-operator created
Error from server (AlreadyExists): error when creating "./operator.yml":
rolebindings.rbac.authorization.k8s.io "system:image-builders" already exists (1)
Error from server (AlreadyExists): error when creating "./operator.yml":
rolebindings.rbac.authorization.k8s.io "system:image-pullers" already exists
```

(1) 您可以忽略 **Error from server (AlreadyExists)** 信息。它们是由 MTC Operator 为早期版本的 OpenShift Container Platform 4 创建资源造成的，这些资源在以后的版本中已提供。

7. 创建 **MigrationController** 对象：

```
$ oc create -f controller.yml
```

8. 验证 MTC Pod 是否正在运行：

```
$ oc get pods -n openshift-migration
```

3.3. 在 OPENSHIFT CONTAINER PLATFORM 4.15 上安装 MTC OPERATOR

您可以使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4.15 上安装 MTC Operator。

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。

流程

1. 在 OpenShift Container Platform Web 控制台中，点击 **Operators → OperatorHub**。
2. 使用 **Filter by keyword** 字段查找 **MTCs Operator**。
3. 选择 **Migration Toolkit for Containers Operator** 并点 **Install**。
4. 点击 **Install**。
   在 **Installed Operators** 页中，**openshift-migration** 项目中会出现状态为 **Succeeded** 的 **Migration Toolkit for Containers Operator**。
5. 点 **Migration Toolkit for Containers Operator**。
6. 在 **Provided APIs** 下，找到 **Migration Controller** 标题，再点 **Create Instance**。
7. 点击 **Create**。
8. 点 **Workloads → Pods** 来验证 MTC pod 正在运行 。

3.4. 代理配置

对于 OpenShift Container Platform 4.1 及更早的版本，您必须在安装 Migration Toolkit for Containers Operator 后，在 **MigrationController** 自定义资源 (CR) 清单中配置代理，因为这些版本不支持集群范围的 **proxy** 对象。

对于 OpenShift Container Platform 4.2 到 4.15，Migration Toolkit for Containers (MTC) 会继承集群范围的代理设置。如果要覆盖集群范围的代理设置，可以更改代理参数。

3.4.1. 直接卷迁移

MTC 1.4.2 中引入了直接卷迁移(DVM)。DVM 只支持一个代理。如果目标集群也位于代理后面，则源集群无法访问目标集群的路由。

如果要从代理后面的源集群执行 DVM，您必须配置一个 TCP 代理，该代理可在传输层进行透明处理，并在不使用自己的 SSL 证书的情况下转发 SSL 连接。Stunnel 代理是此类代理的示例。

3.4.1.1. DVM 的 TCP 代理设置

您可以通过 TCP 代理在源和目标集群之间设置直接连接，并在 **MigrationController** CR 中配置 **stunnel_tcp_proxy** 变量来使用代理：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  stunnel_tcp_proxy: http://username:password@ip:port
```

直接卷迁移(DVM)只支持代理的基本身份验证。此外，DVM 仅适用于可透明地传输 TCP 连接的代理。在 man-in-the-middle 模式中的 HTTP/HTTPS 代理无法正常工作。现有的集群范围的代理可能不支持此行为。因此，DVM 的代理设置意与 MTC 中常见的代理配置不同。

3.4.1.2. 为什么使用 TCP 代理而不是 HTTP/HTTPS 代理？

您可以通过 OpenShift 路由在源和目标集群之间运行 Rsync 来启用 DVM。流量通过 TCP 代理(Stunnel)加密。在源集群上运行的 Stunnel 会启动与目标 Stunnel 的 TLS 连接，并通过加密频道来传输数据。

OpenShift 中的集群范围 HTTP/HTTPS 代理通常在 man-in-the-middle 模式进行配置，其中它们将自己的 TLS 会话与外部服务器协商。但是，这不适用于 Stunnel。Stunnel 要求代理不处理它的 TLS 会话，基本上使代理成为一个透明的隧道，只需按原样转发 TCP 连接。因此，您必须使用 TCP 代理。

3.4.1.3. 已知问题

迁移失败并显示 Upgrade request required 错误

迁移控制器使用 SPDY 协议在远程 pod 中执行命令。如果远程集群位于代理或不支持 SPDY 协议的防火墙后，迁移控制器将无法执行远程命令。迁移失败并显示出错信息 **Upgrade request required**。临时解决方案： 使用支持 SPDY 协议的代理。

除了支持 SPDY 协议外，代理或防火墙还必须将 **Upgrade** HTTP 标头传递给 API 服务器。客户端使用此标头打开与 API 服务器的 websocket 连接。如果代理或防火墙阻止 **Upgrade** 标头，则迁移会失败，并显示出错信息 **Upgrade request required**。临时解决方案：确保代理转发 **Upgrade** 标头。

3.4.2. 为迁移调优网络策略

OpenShift 支持根据集群使用的网络插件，限制使用 *NetworkPolicy* 或 *EgressFirewalls* 的流量。如果任何涉及迁移的源命名空间使用此类机制将网络流量限制到 pod，限制可能会在迁移过程中停止到 Rsync pod 的流量。

在源和目标集群上运行的 rsync pod 必须通过 OpenShift Route 相互连接。可将现有的 *NetworkPolicy* 或 *EgressNetworkPolicy* 对象配置为从这些流量限制自动排除 Rsync pod。

3.4.2.1. NetworkPolicy 配置

3.4.2.1.1. 来自 Rsync pod 的出口流量

如果源或目标命名空间中的 **NetworkPolicy** 配置阻止这种类型的流量，您可以使用 Rsync pod 的唯一标签来允许出口流量从它们传递。以下策略允许来自命名空间中 Rsync pod 的**所有**出口流量：

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-from-rsync-pods
spec:
  podSelector:
    matchLabels:
      owner: directvolumemigration
      app: directvolumemigration-rsync-transfer
  egress:
  - {}
  policyTypes:
  - Egress
```

3.4.2.1.2. 到 Rsync pod 的入口流量

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
```

```
  name: allow-all-egress-from-rsync-pods
spec:
  podSelector:
    matchLabels:
      owner: directvolumemigration
      app: directvolumemigration-rsync-transfer
  ingress:
  - {}
  policyTypes:
  - Ingress
```

3.4.2.2. EgressNetworkPolicy 配置

EgressNetworkPolicy 对象或 *Egress Firewalls* 是 OpenShift 构造，用于阻止离开集群的出口流量。

与 **NetworkPolicy** 对象不同，egress Firewall 在项目级别工作，因为它适用于命名空间中的所有 pod。因此，Rsync pod 的唯一标签不会使只有 Rsync pod 的 Rsync pod 冲突。但是，您可以将源集群或目标集群的 CIDR 范围添加到策略的 *Allow* 规则中，以便可以在两个集群之间设置直接连接。

根据存在 Egress Firewall 的集群，您可以添加其他集群的 CIDR 范围来允许两者间的出口流量：

```
apiVersion: network.openshift.io/v1
kind: EgressNetworkPolicy
metadata:
  name: test-egress-policy
  namespace: <namespace>
spec:
  egress:
  - to:
      cidrSelector: <cidr_of_source_or_target_cluster>
    type: Deny
```

3.4.2.3. 为数据传输选择备用端点

默认情况下，DVM 使用 OpenShift Container Platform 路由作为端点，将 PV 数据传送到目标集群。如果集群拓扑允许，您可以选择其他类型的支持的端点。

对于每个集群，您可以通过在 **MigrationController** CR 中适当的 目标集群上设置 **rsync_endpoint_type** 变量来配置端点：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  rsync_endpoint_type: [NodePort|ClusterIP|Route]
```

3.4.2.4. 为 Rsync pod 配置补充组

当 PVC 使用共享存储时，您可以通过将 supplemental 组添加到 Rsync pod 定义来配置对存储的访问，以便 pod 允许访问：

表 3.2. Rsync pod 的附加组群

变量	类型	Default（默认）	描述
src_supplemental_groups	string	未设置	用于源 Rsync pod 的以逗号分隔的补充组列表
target_supplemental_groups	string	未设置	目标 Rsync pod 的，以逗号分隔的补充组列表

用法示例

可以更新 **MigrationController** CR，以便为这些补充组设置值：

```
spec:
  src_supplemental_groups: "1000,2000"
  target_supplemental_groups: "2000,3000"
```

3.4.3. 配置代理

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。

流程

1. 获取 **MigrationController** CR 清单：

```
$ oc get migrationcontroller <migration_controller> -n openshift-migration
```

2. 更新代理参数：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: <migration_controller>
  namespace: openshift-migration
...
spec:
  stunnel_tcp_proxy: http://<username>:<password>@<ip>:<port> 1
  noProxy: example.com 2
```

1. 用于直接卷迁移的 stunnel 代理 URL。
2. 要排除代理的目标域名、域、IP 地址或其他网络 CIDR 的逗号分隔列表。

在域前面加 **.** 来仅匹配子域。例如： **.y.com** 匹配 **x.y.com**，但不匹配 **y.com**。使用 * 可对所有目的地绕过所有代理。如果您扩展了未包含在安装配置中 **networking.machineNetwork[].cidr** 字段定义的 worker，您必须将它们添加到此列表中，以防止连接问题。

如果未设置 **httpProxy** 和 **httpsProxy** 字段，则此字段将被忽略。

3. 将清单保存为 **migration-controller.yaml**。

4. 应用更新的清单：

```
$ oc replace -f migration-controller.yaml -n openshift-migration
```

如需更多信息，请参阅配置集群范围代理。

3.4.4. 以 root 或非 root 身份运行 Rsync

OpenShift Container Platform 环境默认启用 **PodSecurityAdmission** 控制器。此控制器要求集群管理员通过命名空间标签强制实施 Pod 安全标准。集群中的所有工作负载都应该运行以下 Pod 安全标准级别之一： **Privileged**、**Baseline** 或 **Restricted**。每个集群都有自己的默认策略集。

为了保证在所有环境中成功进行数据传输，MTC 1.7.5 引入了 Rsync pod 中的更改，包括默认以非 root 用户身份运行 Rsync pod。这样可确保即使不一定需要更高特权的工作负载也可以进行数据传输。这个更改是进行的，因为它最适合运行具有最低级别权限的工作负载。

3.4.4.1. 为数据 trannsfer 手动覆盖默认非 root 操作

虽然在大多数情况下，以非 root 用户身份运行 Rsync pod 可以正常工作，但当您以 root 用户身份在源端运行工作负载时，数据传输可能会失败。MTC 提供了为数据传输手动覆盖默认非 root 操作的方法：

- 将所有迁移配置为作为 root 在目标集群上针对所有迁移运行 Rsync pod。
- 对于每个迁移，在目标集群上以 root 用户身份运行 Rsync pod。

在这两种情况下，您必须在迁移前运行具有较高特权的工作负载的命名空间源上设置以下标签：
enforce、**audit** 和 **warn**。

要了解更多有关标签的 Pod Security Admission 和设置值的信息，请参阅 控制 pod 安全准入同步。

3.4.4.2. 将所有迁移的 MigrationController CR 配置为 root 或非 root

默认情况下，Rsync 作为非 root 运行。

在目标集群中，您可以将 **MigrationController** CR 配置为以 root 用户身份运行 Rsync。

流程

- 配置 **MigrationController** CR，如下所示：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  migration_rsync_privileged: true
```

此配置将适用于所有将来的迁移。

3.4.4.3. 将 MigMigration CR 配置为每个迁移的根或非 root

在目标集群中，您可以使用以下非 root 选项将 **MigMigration** CR 配置为以 root 或非 root 身份运行 Rsync：

- 作为特定用户 ID (UID)
- 作为一个特定组 ID (GID)

流程

1. 要以 root 用户身份运行 Rsync，请根据本例配置 **MigMigration** CR：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  runAsRoot: true
```

2. 要将 Rsync 作为特定用户 ID (UID)或特定组 ID (GID)运行，请根据本例配置 **MigMigration** CR：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  runAsUser: 10010001
  runAsGroup: 3
```

3.5. 配置复制存储库

您必须将对象存储配置为用作复制存储库。MTC 将数据从源集群复制到复制存储库，然后从复制存储库复制到目标集群。

MTC 支持使用文件系统和快照数据复制的方法将数据从源集群迁移到目标集群。您可以选择适合于您的环境并受您的存储供应商支持的方法。

MTC 支持以下存储供应商：

- 多云对象网关
- Amazon Web Services S3
- Google Cloud Platform
- Microsoft Azure Blob
- 通用 S3 对象存储，例如 Minio 或 Ceph S3

3.5.1. 先决条件

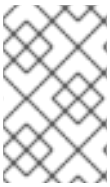
- 所有集群都必须具有对复制存储库的不间断网络访问权限。

- 如果您将代理服务器与内部托管的复制存储库搭配使用，您必须确保代理允许访问复制存储库。

3.5.2. 检索多云对象网关凭证

您必须检索 Multicloud Object Gateway (MCG)凭证和 S3 端点，您需要将 MCG 配置为 MTC 的 Migration Toolkit for Containers (MTC)的复制仓库

您必须检索 Multicloud Object Gateway (MCG)凭证，您需要为 MTC 创建 **Secret** 自定义资源(CR)。



注意

虽然 MCG Operator 已被弃用，但 MCG 插件仍可用于 OpenShift Data Foundation。要下载插件，请浏览 下载 Red Hat OpenShift Data Foundation，并为您的操作系统下载适当的 MCG 插件。

先决条件

- 您必须使用适当的 Red Hat OpenShift Data Foundation 部署指南 部署 OpenShift Data Foundation。

流程

- 通过在 **NooBaa** 自定义资源上运行 **describe** 命令，获取 S3 端点、**AWS_ACCESS_KEY_ID** 和 **AWS_SECRET_ACCESS_KEY**。
  您可以使用这些凭证将 MCG 作为复制存储库来添加。

3.5.3. 配置 Amazon Web Services

您可以将 Amazon Web Services(AWS)S3 对象存储配置为 MTC 的 Migration Toolkit for Containers(MTC)的复制仓库。

先决条件

- 已安装 AWS CLI。
- AWS S3 存储桶必须可以被源和目标集群访问。
- 如果您使用快照复制方法：
  - 您必须有权访问 EC2 Elastic Block Storage (EBS)。
  - 源和目标集群必须位于同一区域。
  - 源和目标集群必须具有相同的存储类。
  - 存储类必须与快照兼容。

流程

1. 设置 **BUCKET** 变量：

```
$ BUCKET=<your_bucket>
```

2. 设置 **REGION** 变量：

```
$ REGION=<your_region>
```

3. 创建 AWS S3 存储桶：

```
$ aws s3api create-bucket \
    --bucket $BUCKET \
    --region $REGION \
    --create-bucket-configuration LocationConstraint=$REGION 1
```

1 **us-east-1** 不支持 **LocationConstraint**。如果您的区域是 **us-east-1**，忽略 **--create-bucket-configuration LocationConstraint=$REGION**。

4. 创建一个 IAM 用户：

```
$ aws iam create-user --user-name velero 1
```

1 如果要使用 Velero 备份具有多个 S3 存储桶的集群，请为每个集群创建一个唯一用户名。

5. 创建 **velero-policy.json** 文件：

```
$ cat > velero-policy.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "arn:aws:s3:::${BUCKET}/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
```

```
            "s3:GetBucketLocation",
            "s3:ListBucketMultipartUploads"
        ],
        "Resource": [
            "arn:aws:s3:::${BUCKET}"
        ]
    }
  ]
}
EOF
```

6. 附加策略，为 **velero** 用户提供所需的最低权限：

```
$ aws iam put-user-policy \
  --user-name velero \
  --policy-name velero \
  --policy-document file://velero-policy.json
```

7. 为 **velero** 用户创建访问密钥：

```
$ aws iam create-access-key --user-name velero
```

输**出示例**

```
{
  "AccessKey": {
        "UserName": "velero",
        "Status": "Active",
        "CreateDate": "2017-07-31T22:24:41.576Z",
        "SecretAccessKey": <AWS_SECRET_ACCESS_KEY>,
        "AccessKeyId": <AWS_ACCESS_KEY_ID>
  }
}
```

记录 **AWS_SECRET_ACCESS_KEY** 和 **AWS_ACCESS_KEY_ID**。您可以使用凭证将 AWS 添加为复制存储库。

3.5.4. 配置 Google Cloud Platform

您可以将 Google Cloud Platform(GCP)存储桶配置为 Migration Toolkit for Containers(MTC)的复制仓库。

先决条件

- 您必须安装了 **gcloud** 和 **gsutil** CLI 工具。详情请查看 Google 云文档。
- GCP 存储桶必须可以被源和目标集群访问。
- 如果您使用快照复制方法：
  - 源和目标集群必须位于同一区域。
  - 源和目标集群必须具有相同的存储类。

- 存储类必须与快照兼容。

流程

1. 登录到 GCP:

```
$ gcloud auth login
```

2. 设置 **BUCKET** 变量：

```
$ BUCKET=<bucket> 1
```

1 指定存储桶名称。

3. 创建存储桶：

```
$ gsutil mb gs://$BUCKET/
```

4. 将 **PROJECT_ID** 变量设置为您的活跃项目：

```
$ PROJECT_ID=$(gcloud config get-value project)
```

5. 创建服务帐户：

```
$ gcloud iam service-accounts create velero \
    --display-name "Velero service account"
```

6. 列出服务帐户：

```
$ gcloud iam service-accounts list
```

7. 设置 **SERVICE_ACCOUNT_EMAIL** 变量，使其与 **email** 值匹配：

```
$ SERVICE_ACCOUNT_EMAIL=$(gcloud iam service-accounts list \
    --filter="displayName:Velero service account" \
    --format 'value(email)')
```

8. 附加策略，为 **velero** 用户提供所需的最低权限：

```
$ ROLE_PERMISSIONS=(
    compute.disks.get
    compute.disks.create
    compute.disks.createSnapshot
    compute.snapshots.get
    compute.snapshots.create
    compute.snapshots.useReadOnly
    compute.snapshots.delete
    compute.zones.get
    storage.objects.create
    storage.objects.delete
    storage.objects.get
```

```
    storage.objects.list
    iam.serviceAccounts.signBlob
)
```

9. 创建 **velero.server** 自定义角色：

```
$ gcloud iam roles create velero.server \
    --project $PROJECT_ID \
    --title "Velero Server" \
    --permissions "$(IFS=","; echo "${ROLE_PERMISSIONS[*]}")"
```

10. 为项目添加 IAM 策略绑定：

```
$ gcloud projects add-iam-policy-binding $PROJECT_ID \
    --member serviceAccount:$SERVICE_ACCOUNT_EMAIL \
    --role projects/$PROJECT_ID/roles/velero.server
```

11. 更新 IAM 服务帐户：

```
$ gsutil iam ch serviceAccount:$SERVICE_ACCOUNT_EMAIL:objectAdmin gs://${BUCKET}
```

12. 将 IAM 服务帐户的密钥保存到当前目录中的 **credentials-velero** 文件中：

```
$ gcloud iam service-accounts keys create credentials-velero \
    --iam-account $SERVICE_ACCOUNT_EMAIL
```

您可以使用 **credentials-velero** 文件将 GCP 添加为复制存储库。

3.5.5. 配置 Microsoft Azure

您可以将 Microsoft Azure Blob 存储容器配置为 Migration Toolkit for Containers(MTC)的复制仓库。

先决条件

- 已安装 Azure CLI。
- Azure Blob 存储容器必须可以被源和目标集群访问。
- 如果您使用快照复制方法：
  - 源和目标集群必须位于同一区域。
  - 源和目标集群必须具有相同的存储类。
  - 存储类必须与快照兼容。

流程

1. 登录到 Azure:

```
$ az login
```

2. 设置 **AZURE_RESOURCE_GROUP** 变量：

```
$ AZURE_RESOURCE_GROUP=Velero_Backups
```

3. 创建 Azure 资源组：

```
$ az group create -n $AZURE_RESOURCE_GROUP --location CentralUS (1)
```

(1) 指定位置。

4. 设置 **AZURE_STORAGE_ACCOUNT_ID** 变量：

```
$ AZURE_STORAGE_ACCOUNT_ID="velero$(uuidgen | cut -d '-' -f5 | tr '[A-Z]' '[a-z]')"
```

5. 创建 Azure 存储帐户：

```
$ az storage account create \
    --name $AZURE_STORAGE_ACCOUNT_ID \
    --resource-group $AZURE_RESOURCE_GROUP \
    --sku Standard_GRS \
    --encryption-services blob \
    --https-only true \
    --kind BlobStorage \
    --access-tier Hot
```

6. 设置 **BLOB_CONTAINER** 变量：

```
$ BLOB_CONTAINER=velero
```

7. 创建 Azure Blob 存储容器：

```
$ az storage container create \
  -n $BLOB_CONTAINER \
  --public-access off \
  --account-name $AZURE_STORAGE_ACCOUNT_ID
```

8. 为 **velero** 创建服务主体和凭证：

```
$ AZURE_SUBSCRIPTION_ID=`az account list --query '[?isDefault].id' -o tsv` \
  AZURE_TENANT_ID=`az account list --query '[?isDefault].tenantId' -o tsv` \
  AZURE_CLIENT_SECRET=`az ad sp create-for-rbac --name "velero" \
  --role "Contributor" --query 'password' -o tsv` \
  AZURE_CLIENT_ID=`az ad sp list --display-name "velero" \
  --query '[0].appId' -o tsv`
```

9. 在 **credentials-velero** 文件中保存服务主体的凭证：

```
$ cat << EOF > ./credentials-velero
AZURE_SUBSCRIPTION_ID=${AZURE_SUBSCRIPTION_ID}
AZURE_TENANT_ID=${AZURE_TENANT_ID}
AZURE_CLIENT_ID=${AZURE_CLIENT_ID}
AZURE_CLIENT_SECRET=${AZURE_CLIENT_SECRET}
```

```
AZURE_RESOURCE_GROUP=${AZURE_RESOURCE_GROUP}
AZURE_CLOUD_NAME=AzurePublicCloud
EOF
```

您可以使用 **credentials-velero** 文件将 Azure 添加为复制存储库。

3.5.6. 其他资源

- MTC 工作流
- 关于数据复制方法
- 在 MTC web 控制台中添加复制存储库

3.6. 卸载 MTC 并删除资源

您可以卸载 MTC，并删除其资源来清理集群。

注意

删除 **velero** CRD 会从集群中移除 Velero。

先决条件

- 您必须以具有 **cluster-admin** 权限的用户身份登录。

流程

1. 删除所有集群中的 **MigrationController** 自定义资源 (CR)：

```
$ oc delete migrationcontroller <migration_controller>
```

2. 使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4 上卸载 MTC Operator。
3. 运行以下命令，删除所有集群中的集群范围资源：
   - **migration** 自定义资源定义 (CRDs)：

```
$ oc delete $(oc get crds -o name | grep 'migration.openshift.io')
```

   - **Velero** CRD：

```
$ oc delete $(oc get crds -o name | grep 'velero')
```

   - **migration** 集群角色：

```
$ oc delete $(oc get clusterroles -o name | grep 'migration.openshift.io')
```

   - **migration-operator** 集群角色：

```
$ oc delete clusterrole migration-operator
```

   - **velero** 集群角色：

```
$ oc delete $(oc get clusterroles -o name | grep 'velero')
```

- **migration** 集群角色绑定：

```
$ oc delete $(oc get clusterrolebindings -o name | grep 'migration.openshift.io')
```

- **migration-operator** 集群角色绑定：

```
$ oc delete clusterrolebindings migration-operator
```

- **velero** 集群角色绑定：

```
$ oc delete $(oc get clusterrolebindings -o name | grep 'velero')
```

第 4 章 在受限网络环境中安装 MTC

您可以通过执行以下步骤在受限网络环境中的 OpenShift Container Platform 4 上安装 MTC：

1. 创建一个镜像的 Operator 目录。
   此过程会创建一个 **mapping.txt** 文件，其中包含 **registry.redhat.io** 镜像和您的镜像 registry 镜像之间的映射。**mapping.txt** 文件是在 OpenShift Container Platform 4.2 到 4.5 源集群中安装 *旧的* MTC Operator 所需要的。

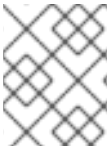
2. 使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4.15 目标集群上安装 MTC。
   默认情况下，MTC web 控制台和 **Migration Controller** pod 在目标集群中运行。您可以配置 **Migration Controller** 自定义资源清单在远程集群中运行 MTC web 控制台和 **Migration Controller** pod。

3. 在源集群中安装 MTC Operator:

   - OpenShift Container Platform 4.6 或更高版本： 使用 Operator Lifecycle Manager 安装 MTC Operator。

   - OpenShift Container Platform 4.2 到 4.5: 使用命令行界面安装传统的 MTC Operator。

4. 配置对象存储，以用作复制存储库。



注意

要在 OpenShift Container Platform 3 上安装 MTC，请参阅在 OpenShift Container Platform 3 上安装旧的 MTC。

要卸载 MTC，请参阅卸载 MTC 并删除资源。

4.1. 兼容性指南

您必须安装与 OpenShift Container Platform 版本兼容的 MTC。

定义

旧平台
OpenShift Container Platform 4.5 及更早版本。

现代平台
OpenShift Container Platform 4.6 及更新的版本。

旧 Operator
针对传统平台设计的 MTC Operator。

现代 operator
针对现代平台设计的 MTC Operator。

控制集群
运行 MTC 控制器和 GUI 的集群。

远程集群
运行 Velero 的迁移的源或目标集群。Control Cluster 通过 Velero API 与远程集群通信，以驱动迁移。

您必须使用兼容的 MTC 版本来迁移 OpenShift Container Platform 集群。要使迁移成功源集群和目标集群，必须使用相同的 MTC 版本。

MTC 1.7 支持从 OpenShift Container Platform 3.11 迁移到 4.9。

MTC 1.8 仅支持从 OpenShift Container Platform 4.10 及更新的版本进行迁移。

表 4.1. MTC 兼容性：从传统或现代平台迁移

详情	OpenShift Container Platform 3.11	OpenShift Container Platform 4.0 到 4.5	OpenShift Container Platform 4.6 到 4.9	OpenShift Container Platform 4.10 或更高版本
稳定 MTC 版本	MTC v.1.7.*z*	MTC v.1.7.*z*	MTC v.1.7.*z*	MTC v.1.8.*z*
安装		旧版 MTC v.1.7.*z* operator：使用 **operator.yml** 文件手动安装。 [**重要信息**] 此集群不能是控制集群。	使用 OLM 安装，发行频道 **release-v1.7**	使用 OLM 安装，发行频道 **release-v1.8**

在某些情况下，网络的限制可能会阻止现代集群连接到迁移中需要涉及的其他集群。例如，当从内部的 OpenShift Container Platform 3.11 集群迁移到云环境中的现代 OpenShift Container Platform 集群时，，现代集群无法连接到 OpenShift Container Platform 3.11 集群。

在 MTC v.1.7.*z* 中，如果其中一个远程集群因为网络限制而无法与控制集群通信，请使用 **crane tunnel-api** 命令。

对于稳定（stable）的 MTC 发行版本，虽然您应该始终将最现代化的集群指定为控制集群，但是在这种情况下，可能需要将旧的集群指定为控制集群，并将工作负载推送到远程集群。

4.2. 在 OPENSHIFT CONTAINER PLATFORM 4.15 上安装 MTC OPERATOR

您可以使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4.15 上安装 MTC Operator。

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。
- 您必须从本地 registry 中的镜像创建 Operator 目录。

流程

1. 在 OpenShift Container Platform Web 控制台中，点击 **Operators → OperatorHub**。
2. 使用 **Filter by keyword** 字段查找 **MTCs Operator**。
3. 选择 **Migration Toolkit for Containers Operator** 并点 **Install**。
4. 点击 **Install**。
   在 **Installed Operators** 页中，**openshift-migration** 项目中会出现状态为 **Succeeded** 的 **Migration Toolkit for Containers Operator**。

5. 点 **Migration Toolkit for Containers Operator**。
6. 在 **Provided APIs** 下，找到 **Migration Controller** 标题，再点 **Create Instance**。
7. 点击 **Create**。
8. 点 **Workloads → Pods** 来验证 MTC pod 正在运行 。

4.3. 在 OPENSHIFT CONTAINER PLATFORM 4.2 到 4.5 上安装旧的 MTC OPERATOR

您可以在 OpenShift Container Platform 版本 4.2 到 4.5 中手动安装旧的 MTC Operator。

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。
- 您必须有权访问 **registry.redhat.io**。
- 必须安装 **podman** 。
- 您必须有一个有网络访问权限的 Linux 工作站才能从 **registry.redhat.io** 下载文件。
- 您必须创建 Operator 目录的镜像镜像。
- 您需要通过镜像的 Operator 目录在 OpenShift Container Platform 4.15 上安装 Migration Toolkit for Containers Operator。

流程

1. 使用您的红帽客户门户网站账户登陆到 **registry.redhat.io**：

```
$ podman login registry.redhat.io
```

2. 输入以下命令下载 **operator.yml** 文件：

```
podman cp $(podman create registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-operator:v1.7):/operator.yml ./
```

3. 输入以下命令下载 **controller.yml** 文件：

```
podman cp $(podman create registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-operator:v1.7):/controller.yml ./
```

4. 运行以下命令来获取 Operator 镜像映射：

```
$ grep openshift-migration-legacy-rhel8-operator ./mapping.txt | grep rhmtc
```

mapping.txt 文件是在对 Operator 目录进行镜像时创建的。输出显示了 **registry.redhat.io** 镜像和您的镜像 registry 镜像之间的映射。

输**出示例**

```
registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-
operator@sha256:468a6126f73b1ee12085ca53a312d1f96ef5a2ca03442bcb63724af5e2614e8
a=<registry.apps.example.com>/rhmtc/openshift-migration-legacy-rhel8-operator
```

5. 在 **operator.yml** 文件中，为 **ansible** 和 **operator** 容器更新 **image** 值，并更新 **REGISTRY** 值：

```
containers:
  - name: ansible
    image: <registry.apps.example.com>/rhmtc/openshift-migration-legacy-rhel8-
operator@sha256:
<468a6126f73b1ee12085ca53a312d1f96ef5a2ca03442bcb63724af5e2614e8a> 1
...
  - name: operator
    image: <registry.apps.example.com>/rhmtc/openshift-migration-legacy-rhel8-
operator@sha256:
<468a6126f73b1ee12085ca53a312d1f96ef5a2ca03442bcb63724af5e2614e8a> 2
...
    env:
    - name: REGISTRY
      value: <registry.apps.example.com> 3
```

1 2 指定您的镜像 registry 和 Operator 镜像的 **sha256** 值。

3 指定您的镜像 registry。

6. 登录您的 OpenShift Container Platform 源集群。

7. 创建 MTC Operator 对象的 Migration Toolkit:

```
$ oc create -f operator.yml
```

输**出示例**

```
namespace/openshift-migration created
rolebinding.rbac.authorization.k8s.io/system:deployers created
serviceaccount/migration-operator created
customresourcedefinition.apiextensions.k8s.io/migrationcontrollers.migration.openshift.io
created
role.rbac.authorization.k8s.io/migration-operator created
rolebinding.rbac.authorization.k8s.io/migration-operator created
clusterrolebinding.rbac.authorization.k8s.io/migration-operator created
deployment.apps/migration-operator created
Error from server (AlreadyExists): error when creating "./operator.yml":
rolebindings.rbac.authorization.k8s.io "system:image-builders" already exists 1
Error from server (AlreadyExists): error when creating "./operator.yml":
rolebindings.rbac.authorization.k8s.io "system:image-pullers" already exists
```

1 您可以忽略 **Error from server (AlreadyExists)** 信息。它们是由 MTC Operator 为早期版本的 OpenShift Container Platform 4 创建资源造成的，这些资源在以后的版本中已提供。

8. 创建 **MigrationController** 对象：

```
$ oc create -f controller.yml
```

9. 验证 MTC Pod 是否正在运行：

```
$ oc get pods -n openshift-migration
```

4.4. 代理配置

对于 OpenShift Container Platform 4.1 及更早的版本，您必须在安装 Migration Toolkit for Containers Operator 后，在 **MigrationController** 自定义资源 (CR) 清单中配置代理，因为这些版本不支持集群范围的 **proxy** 对象。

对于 OpenShift Container Platform 4.2 到 4.15，Migration Toolkit for Containers (MTC) 会继承集群范围的代理设置。如果要覆盖集群范围的代理设置，可以更改代理参数。

4.4.1. 直接卷迁移

MTC 1.4.2 中引入了直接卷迁移(DVM)。DVM 只支持一个代理。如果目标集群也位于代理后面，则源集群无法访问目标集群的路由。

如果要从代理后面的源集群执行 DVM，您必须配置一个 TCP 代理，该代理可在传输层进行透明处理，并在不使用自己的 SSL 证书的情况下转发 SSL 连接。Stunnel 代理是此类代理的示例。

4.4.1.1. DVM 的 TCP 代理设置

您可以通过 TCP 代理在源和目标集群之间设置直接连接，并在 **MigrationController** CR 中配置 **stunnel_tcp_proxy** 变量来使用代理：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  stunnel_tcp_proxy: http://username:password@ip:port
```

直接卷迁移(DVM)只支持代理的基本身份验证。此外，DVM 仅适用于可透明地传输 TCP 连接的代理。在 man-in-the-middle 模式中的 HTTP/HTTPS 代理无法正常工作。现有的集群范围的代理可能不支持此行为。因此，DVM 的代理设置意与 MTC 中常见的代理配置不同。

4.4.1.2. 为什么使用 TCP 代理而不是 HTTP/HTTPS 代理？

您可以通过 OpenShift 路由在源和目标集群之间运行 Rsync 来启用 DVM。流量通过 TCP 代理(Stunnel)加密。在源集群上运行的 Stunnel 会启动与目标 Stunnel 的 TLS 连接，并通过加密频道来传输数据。

OpenShift 中的集群范围 HTTP/HTTPS 代理通常在 man-in-the-middle 模式进行配置，其中它们将自己的 TLS 会话与外部服务器协商。但是，这不适用于 Stunnel。Stunnel 要求代理不处理它的 TLS 会话，基本上使代理成为一个透明的隧道，只需按原样转发 TCP 连接。因此，您必须使用 TCP 代理。

4.4.1.3. 已知问题

迁移失败并显示 Upgrade request required 错误

迁移控制器使用 SPDY 协议在远程 pod 中执行命令。如果远程集群位于代理或不支持 SPDY 协议的防火墙后，迁移控制器将无法执行远程命令。迁移失败并显示出错信息 **Upgrade request required**。临时解决方案： 使用支持 SPDY 协议的代理。

除了支持 SPDY 协议外，代理或防火墙还必须将 **Upgrade** HTTP 标头传递给 API 服务器。客户端使用此标头打开与 API 服务器的 websocket 连接。如果代理或防火墙阻止 **Upgrade** 标头，则迁移会失败，并显示出错信息 **Upgrade request required**。临时解决方案：确保代理转发 **Upgrade** 标头。

4.4.2. 为迁移调优网络策略

OpenShift 支持根据集群使用的网络插件，限制使用 *NetworkPolicy* 或 *EgressFirewalls* 的流量。如果任何涉及迁移的源命名空间使用此类机制将网络流量限制到 pod，限制可能会在迁移过程中停止到 Rsync pod 的流量。

在源和目标集群上运行的 rsync pod 必须通过 OpenShift Route 相互连接。可将现有的 *NetworkPolicy* 或 *EgressNetworkPolicy* 对象配置为从这些流量限制自动排除 Rsync pod。

4.4.2.1. NetworkPolicy 配置

4.4.2.1.1. 来自 Rsync pod 的出口流量

如果源或目标命名空间中的 **NetworkPolicy** 配置阻止这种类型的流量，您可以使用 Rsync pod 的唯一标签来允许出口流量从它们传递。以下策略允许来自命名空间中 Rsync pod 的**所有**出口流量：

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-from-rsync-pods
spec:
  podSelector:
    matchLabels:
      owner: directvolumemigration
      app: directvolumemigration-rsync-transfer
  egress:
  - {}
  policyTypes:
  - Egress
```

4.4.2.1.2. 到 Rsync pod 的入口流量

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-from-rsync-pods
spec:
  podSelector:
    matchLabels:
      owner: directvolumemigration
      app: directvolumemigration-rsync-transfer
  ingress:
  - {}
  policyTypes:
  - Ingress
```

4.4.2.2. EgressNetworkPolicy 配置

EgressNetworkPolicy 对象或 *Egress Firewalls* 是 OpenShift 构造，用于阻止离开集群的出口流量。

与 **NetworkPolicy** 对象不同，egress Firewall 在项目级别工作，因为它适用于命名空间中的所有 pod。因此，Rsync pod 的唯一标签不会使只有 Rsync pod 的 Rsync pod 冲突。但是，您可以将源集群或目标集群的 CIDR 范围添加到策略的 *Allow* 规则中，以便可以在两个集群之间设置直接连接。

根据存在 Egress Firewall 的集群，您可以添加其他集群的 CIDR 范围来允许两者间的出口流量：

```
apiVersion: network.openshift.io/v1
kind: EgressNetworkPolicy
metadata:
  name: test-egress-policy
  namespace: <namespace>
spec:
  egress:
  - to:
      cidrSelector: <cidr_of_source_or_target_cluster>
    type: Deny
```

4.4.2.3. 为**数据**传输选择备**用端点**

默认情况下，DVM 使用 OpenShift Container Platform 路由作为端点，将 PV 数据传送到目标集群。如果集群拓扑允许，您可以选择其他类型的支持的端点。

对于每个集群，您可以通过在 **MigrationController** CR 中适当的 **目标集群上设置 rsync_endpoint_type** 变量来配置端点：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  rsync_endpoint_type: [NodePort|ClusterIP|Route]
```

4.4.2.4. 为 **Rsync pod 配置**补**充**组

当 PVC 使用共享存储时，您可以通过将 supplemental 组添加到 Rsync pod 定义来配置对存储的访问，以便 pod 允许访问：

表 4.2. Rsync pod 的附加组群

变量	类型	Default（默认）	描述
src_supplemental_groups	string	未设置	用于源 Rsync pod 的以逗号分隔的补充组列表
target_supplemental_groups	string	未设置	目标 Rsync pod 的，以逗号分隔的补充组列表

用法示例

可以更新 **MigrationController** CR，以便为这些补充组设置值：

```
spec:
  src_supplemental_groups: "1000,2000"
  target_supplemental_groups: "2000,3000"
```

4.4.3. 配置代理

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。

流程

1. 获取 **MigrationController** CR 清单：

```
$ oc get migrationcontroller <migration_controller> -n openshift-migration
```

2. 更新代理参数：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: <migration_controller>
  namespace: openshift-migration
...
spec:
  stunnel_tcp_proxy: http://<username>:<password>@<ip>:<port> 1
  noProxy: example.com 2
```

1. 用于直接卷迁移的 stunnel 代理 URL。
2. 要排除代理的目标域名、域、IP 地址或其他网络 CIDR 的逗号分隔列表。

   在域前面加 **.** 来仅匹配子域。例如：**.y.com** 匹配 **x.y.com**，但不匹配 **y.com**。使用 * 可对所有目的地绕过所有代理。如果您扩展了未包含在安装配置中 **networking.machineNetwork[].cidr** 字段定义的 worker，您必须将它们添加到此列表中，以防止连接问题。

   如果未设置 **httpProxy** 和 **httpsProxy** 字段，则此字段将被忽略。

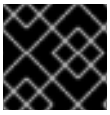
3. 将清单保存为 **migration-controller.yaml**。

4. 应用更新的清单：

```
$ oc replace -f migration-controller.yaml -n openshift-migration
```

如需更多信息，请参阅配置集群范围代理。

4.5. 以 ROOT 或非 ROOT 身份运行 RSYNC



重要

本节仅在使用 OpenShift API 而不是 Web 控制台时应用。

OpenShift 环境默认启用 **PodSecurityAdmission** 控制器。此控制器要求集群管理员通过命名空间标签强制实施 Pod 安全标准。集群中的所有工作负载都应该运行以下 Pod 安全标准级别之一：**Privileged**、**Baseline** 或 **Restricted**。每个集群都有自己的默认策略集。

为了保证在所有环境中成功进行数据传输，MTC 1.7.5 引入了 Rsync pod 中的更改，包括默认以非 root 用户身份运行 Rsync pod。这样可确保即使不一定需要更高特权的工作负载也可以进行数据传输。这个更改是进行的，因为它最适合运行具有最低级别权限的工作负载。

为**数据 trannsfer 手动覆盖默认非 root 操作**
虽然在大多数情况下，以非 root 用户身份运行 Rsync pod 可以正常工作，但当您以 root 用户身份在源端运行工作负载时，数据传输可能会失败。MTC 提供了为数据传输手动覆盖默认非 root 操作的方法：

- 将所有迁移配置为作为 root 在目标集群上针对所有迁移运行 Rsync pod。
- 对于每个迁移，在目标集群上以 root 用户身份运行 Rsync pod。

在这两种情况下，您必须在迁移前运行具有较高权限的工作负载的命名空间源上设置以下标签：**enforce**、**audit** 和 **warn**。

要了解更多有关标签的 Pod Security Admission 和设置值的信息，请参阅 控制 pod 安全准入同步。

4.5.1. 将所有迁移的 MigrationController CR 配置为 root 或非 root

默认情况下，Rsync 作为非 root 运行。

在目标集群中，您可以将 **MigrationController** CR 配置为以 root 用户身份运行 Rsync。

流程

- 配置 **MigrationController** CR，如下所示：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  migration_rsync_privileged: true
```

此配置将适用于所有将来的迁移。

4.5.2. 将 MigMigration CR 配置为每个迁移的根或非 root

在目标集群中，您可以使用以下非 root 选项将 **MigMigration** CR 配置为以 root 或非 root 身份运行 Rsync：

- 作为特定用户 ID (UID)
- 作为一个特定组 ID (GID)

流程

1. 要以 root 用户身份运行 Rsync，请根据本例配置 **MigMigration** CR：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  runAsRoot: true
```

2. 要将 Rsync 作为特定用户 ID (UID)或特定组 ID (GID)运行，请根据本例配置 **MigMigration** CR：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  runAsUser: 10010001
  runAsGroup: 3
```

4.6. 配置复制存储库

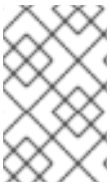
Multicloud 对象网关是受限网络环境唯一支持的选项。

MTC 支持使用文件系统和快照数据复制的方法将数据从源集群迁移到目标集群。您可以选择适合于您的环境并受您的存储供应商支持的方法。

4.6.1. 先决条件

- 所有集群都必须具有对复制存储库的不间断网络访问权限。
- 如果您将代理服务器与内部托管的复制存储库搭配使用，您必须确保代理允许访问复制存储库。

4.6.2. 检索多云对象网关凭证



注意

虽然 MCG Operator 已被弃用，但 MCG 插件仍可用于 OpenShift Data Foundation。要下载插件，请浏览 下载 Red Hat OpenShift Data Foundation，并为您的操作系统下载适当的 MCG 插件。

先决条件

- 您必须使用适当的 Red Hat OpenShift Data Foundation 部署指南 部署 OpenShift Data Foundation。

4.6.3. 其他资源

流程

- Red Hat OpenShift Data Foundation 文档中的断开连接的环境。
- MTC 工作流
- 关于数据复制方法
- 在 MTC web 控制台中添加复制存储库

4.7. 卸载 MTC 并删除资源

您可以卸载 MTC，并删除其资源来清理集群。

注意

删除 **velero** CRD 会从集群中移除 Velero。

先决条件

- 您必须以具有 **cluster-admin** 权限的用户身份登录。

流程

1. 删除所有集群中的 **MigrationController** 自定义资源 (CR)：

```
$ oc delete migrationcontroller <migration_controller>
```

2. 使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4 上卸载 MTC Operator。
3. 运行以下命令，删除所有集群中的集群范围资源：
   - **migration** 自定义资源定义 (CRDs)：

```
$ oc delete $(oc get crds -o name | grep 'migration.openshift.io')
```

   - **Velero** CRD：

```
$ oc delete $(oc get crds -o name | grep 'velero')
```

   - **migration** 集群角色：

```
$ oc delete $(oc get clusterroles -o name | grep 'migration.openshift.io')
```

   - **migration-operator** 集群角色：

```
$ oc delete clusterrole migration-operator
```

   - **velero** 集群角色：

```
$ oc delete $(oc get clusterroles -o name | grep 'velero')
```

   - **migration** 集群角色绑定：

```
$ oc delete $(oc get clusterrolebindings -o name | grep 'migration.openshift.io')
```

- **migration-operator** 集群角色绑定：

```
$ oc delete clusterrolebindings migration-operator
```

- **velero** 集群角色绑定：

```
$ oc delete $(oc get clusterrolebindings -o name | grep 'velero')
```

第 5 章 升级 MTC

您可以使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4.15 上升级 MTC。

您可以通过重新安装 Containers Operator 的传统 Migration Toolkit for Containers Operator，在 OpenShift Container Platform 4.5 及更早的版本上升级 MTC。

重要

如果要升级到 MTC 1.3，您必须执行额外步骤来更新 **MigPlan** 自定义资源（CR）。

5.1. 在 OPENSHIFT CONTAINER PLATFORM 4.15 中升级 MTC

您可以使用 Operator Lifecycle Manager 在 OpenShift Container Platform 4.15 上升级 MTC。

重要

当使用 Operator Lifecycle Manager 升级 MTC 时，必须使用受支持的迁移路径。

迁移路径

- 从 OpenShift Container Platform 3 迁移到 OpenShift Container Platform 4 需要旧的 MTC Operator 和 MTC 1.7.x。
- 不支持从 MTC 1.7.x 迁移到 MTC 1.8.x。
- 您必须使用 MTC 1.7.x 来迁移使用 OpenShift Container Platform 4.9 或更早版本源的任何内容。
  - MTC 1.7.x 必须在源和目标中使用。
- MTC 1.8.x 仅支持从 OpenShift Container Platform 4.10 或更高版本迁移到 OpenShift Container Platform 4.10 或更高版本。对于仅涉及集群版本 4.10 或更高版本的迁移，可以使用 1.7.x 或 1.8.x。但是，它必须与源和目标上的 MTC 版本相同。
  - 不支持从源 MTC 1.7.x 迁移到目标 MTC 1.8.x。
  - 不支持从源 MTC 1.8.x 迁移到目标 MTC 1.7.x。
  - 支持从源 MTC 1.7.x 迁移到目标 MTC 1.7.x。
  - 支持从源 MTC 1.8.x 迁移到目标 MTC 1.8.x

先决条件

- 您必须以具有 **cluster-admin** 权限的用户身份登录。

流程

1. 在 OpenShift Container Platform 控制台中导航至 **Operators → Installed Operators**。处于待定升级的 operator 会显示 **Upgrade available** 状态。
2. 点 **Migration Toolkit for Containers Operator**。
3. 点 **Subscription** 标签页。任何需要批准的升级都会在 **Upgrade Status** 旁边显示。例如：它可能会显示 **1 requires approval**。

4. 点 1 requires approval，然后点 Preview Install Plan。
5. 查看列出可用于升级的资源，并点 Approve。
6. 返回 Operators → Installed Operators 页面来监控升级的过程。完成后，状态会变为 Succeeded 和 Up to date。
7. 点 Workloads → Pods 来验证 MTC pod 正在运行 。

5.2. 将 MTC 升级到 1.8.0

要将 MTC 升级到 1.8.0，请完成以下步骤。

流程

1. 使用以下方法之一确定要升级的订阅名称和当前频道：
   - 运行以下命令确定订阅名称和频道：

     ```
     $ oc -n openshift-migration get sub
     ```

     输出示例

     ```
     NAME                                                                PACKAGE              SOURCE
     CHANNEL
     mtc-operator                                                         mtc-operator         mtc-operator-
     catalog   release-v1.7
     redhat-oadp-operator-stable-1.0-mtc-operator-catalog-openshift-marketplace   redhat-
     oadp-operator   mtc-operator-catalog   stable-1.0
     ```

   - 或者运行以下命令来返回 JSON 中的订阅名称和频道：

     ```
     $ oc -n openshift-migration get sub -o json | jq -r '.items[] | { name: .metadata.name,
     package: .spec.name, channel: .spec.channel }'
     ```

     输出示例

     ```
     {
       "name": "mtc-operator",
       "package": "mtc-operator",
       "channel": "release-v1.7"
     }
     {
       "name": "redhat-oadp-operator-stable-1.0-mtc-operator-catalog-openshift-marketplace",
       "package": "redhat-oadp-operator",
       "channel": "stable-1.0"
     }
     ```

2. 对于每个订阅，运行以下命令来从 MTC 1.7 频道迁移到 MTC 1.8 频道：

   ```
   $ oc -n openshift-migration patch subscription mtc-operator --type merge --patch '{"spec":
   {"channel": "release-v1.8"}}'
   ```

输**出示例**

```
subscription.operators.coreos.com/mtc-operator patched
```

5.2.1. 将 OADP 1.0 升级到 1.2 for Containers 1.8.0

要将 OADP 1.0 升级到 1.2 for Containers 1.8.0，请完成以下步骤。

流程

- 对于每个订阅，运行以下命令，将 OADP operator 从 OADP 1.0 修补到 OADP 1.2：

```
$ oc -n openshift-migration patch subscription redhat-oadp-operator-stable-1.0-mtc-operator-catalog-openshift-marketplace --type merge --patch '{"spec": {"channel":"stable-1.2"}}'
```

注意

指示用户特定返回的 **NAME** 值分别用于安装 MTC 和 OADP 的部分。

输**出示例**

```
subscription.operators.coreos.com/redhat-oadp-operator-stable-1.0-mtc-operator-catalog-openshift-marketplace patched
```

注意

返回的值与 **redhat-oadp-operator-stable-1.0-mtc-operator-catalog-openshift-marketplace** 类似，在本示例中使用。

  - 如果 **installPlanApproval** 参数设置为 **Automatic**，Operator Lifecycle Manager (OLM)将开始升级过程。
  - 如果将 **installPlanApproval** 参数设置为 **Manual**，则必须在 OLM 开始升级前批准每个 **installPlan**。

验证

1. 运行以下命令，验证 OLM 是否已完成 OADP 和 MTC 的升级：

```
$ oc -n openshift-migration get subscriptions.operators.coreos.com mtc-operator -o json | jq '.status | (."state"=="AtLatestKnown")'
```

2. 当返回 **true** 值时，运行以下命令来验证每个订阅使用的频道：

```
$ oc -n openshift-migration get sub -o json | jq -r '.items[] | {name: .metadata.name, channel: .spec.channel }'
```

输**出示例**

```
{
  "name": "mtc-operator",
```

```
  "channel": "release-v1.8"
}
{
  "name": "redhat-oadp-operator-stable-1.0-mtc-operator-catalog-openshift-marketplace",
  "channel": "stable-1.2"
}
```

Confirm that the `mtc-operator.v1.8.0` and `oadp-operator.v1.2.x` packages are installed by running the following command:

```
$ oc -n openshift-migration get csv
```

输**出示例**

```
NAME                 DISPLAY                            VERSION   REPLACES                 PHASE
mtc-operator.v1.8.0      Migration Toolkit for Containers Operator   1.8.0     mtc-operator.v1.7.13     Succeeded
oadp-operator.v1.2.2     OADP Operator                       1.2.2     oadp-operator.v1.0.13    Succeeded
```

5.3. 在 OPENSHIFT CONTAINER PLATFORM 版本 4.2 中将 MTC 升级到 4.5

您可以通过手动安装旧的 MTC Operator，将 OpenShift Container Platform 版本 4.2 上的 MTC 升级到 4.5。

先决条件

- 您必须以具有 **cluster-admin** 权限的用户身份登录。
- 您必须有权访问 **registry.redhat.io**。
- 必须安装 **podman** 。

流程

1. 输入以下命令，使用您的红帽客户门户网站凭证登录到 **registry.redhat.io** ：

```
$ podman login registry.redhat.io
```

2. 输入以下命令下载 **operator.yml** 文件：

```
$ podman cp $(podman create \
  registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-operator:v1.8):/operator.yml ./
```

3. 输入以下命令替换 Containers Operator 的 Migration Toolkit：

```
$ oc replace --force -f operator.yml
```

4. 输入以下命令将 **migration-operator** 部署扩展到 **0** 以停止部署：

```
$ oc scale -n openshift-migration --replicas=0 deployment/migration-operator
```

5. 输入以下命令将 **migration-operator** 部署扩展到 **1** 以启动部署并应用更改：

```
$ oc scale -n openshift-migration --replicas=1 deployment/migration-operator
```

6. 输入以下命令验证 **migration-operator** 是否已升级：

```
$ oc -o yaml -n openshift-migration get deployment/migration-operator | grep image: | awk -F
":" '{ print $NF }'
```

7. 输入以下命令下载 **controller.yml** 文件：

```
$ podman cp $(podman create \
  registry.redhat.io/rhmtc/openshift-migration-legacy-rhel8-operator:v1.8):/controller.yml ./
```

8. 运行以下命令来创建 **migration-controller** 对象：

```
$ oc create -f controller.yml
```

9. 输入以下命令验证 MTC pod 是否正在运行：

```
$ oc get pods -n openshift-migration
```

5.4. 将 MTC 1.3 升级到 1.8

如果要将 MTC 版本 1.3.x 升级到 1.8，您必须更新运行 **MigrationController** Pod 的集群中的 **MigPlan** 自定义资源(CR)清单。

由于 MTC 1.3 中不存在 **indirectImageMigration** 和 **indirectVolumeMigration** 参数，它们在 1.4 版中的默认值会为 **false**，这意味着启用了直接镜像迁移和直接卷迁移。由于没有满足直接迁移要求，迁移计划无法变为 **Ready** 状态，除非将这些参数值改为 **true**。

重要

- 从 OpenShift Container Platform 3 迁移到 OpenShift Container Platform 4 需要旧的 MTC Operator 和 MTC 1.7.x。
- 将 MTC 1.7.x 升级到 1.8.x 需要手动将 OADP 频道从 **stable-1.0** 更新至 **stable-1.2**，以便成功完成从 1.7.x 升级到 1.8.x。

先决条件

- 您必须以具有 **cluster-admin** 权限的用户身份登录。

流程

1. 登录到运行 **MigrationController** Pod 的集群。
2. 获取 **MigPlan** CR 清单：

```
$ oc get migplan <migplan> -o yaml -n openshift-migration
```

3. 更新以下参数值，并将文件保存为 **migplan.yaml**：

```
...
spec:
  indirectImageMigration: true
  indirectVolumeMigration: true
```

4. 替换 **MigPlan** CR 清单以应用更改：

```
$ oc replace -f migplan.yaml -n openshift-migration
```

5. 获取更新的 **MigPlan** CR 清单以验证更改：

```
$ oc get migplan <migplan> -o yaml -n openshift-migration
```

第 6 章 预迁移检查列表

在使用 Migration Toolkit for Containers（MTC）迁移应用程序工作负载前，请查看以下检查列表。

6.1. 集群健康检查清单

❑ 集群满足特定平台和安装方法（例如在裸机上）的最低硬件要求。

❑ 满足所有 MTC 的先决条件。

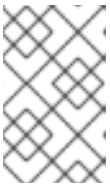
❑ 所有节点都有一个有效的 OpenShift Container Platform 订阅。

❑ 已验证节点健康状况。

❑ 身份提供程序可以正常工作。

❑ 迁移网络的最小吞吐量为 10 Gbps。

❑ 集群有足够的资源进行迁移。



注意

集群需要额外的内存、CPU 和存储，以便在正常工作负载之上运行迁移。实际的资源要求取决于单个迁移计划中迁移的 Kubernetes 资源数量。您必须在非生产环境中测试迁移，以便估计资源要求。

❑ 已使用 **fio** 检查了集群的 etcd 磁盘性能。

6.2. 源集群检查列表

❑ 您已通过运行以下命令检查是否有异常配置的处于 **Terminating** 状态的持久性卷（PV）：

```
$ oc get pv
```

❑ 您已通过运行以下命令检查了状态不是 **Running** 或 **Completed** 的 pod：

```
$ oc get pods --all-namespaces | egrep -v 'Running | Completed'
```

❑ 您已通过运行以下命令来检查有高重启次数的 pod：

```
$ oc get pods --all-namespaces --field-selector=status.phase=Running \
  -o json | jq '.items[]|select(any( .status.containerStatuses[]; \
  .restartCount > 3))|.metadata.name'
```

即使 pod 处于 **Running** 状态，具有高的重启次数可能表示底层有问题。

❑ 集群证书在迁移过程中是有效的。

❑ 您已通过运行以下命令检查是否有待处理的证书签名请求：

```
$ oc get csr -A | grep pending -i
```

❑ registry 使用推荐的存储类型。

- ❑ 您可以将镜像读取和写入到 registry。
- ❑ etcd 集群是健康的。
- ❑ 源集群中的平均 API 服务器响应时间小于 50 ms。

6.3. 目标集群清单

- ❑ 集群具有访问外部服务（如数据库、源代码存储库、容器镜像 registry 和 CI/CD 工具）的正确网络配置和权限。
- ❑ 使用集群提供的服务的外部应用程序和服务具有访问集群的正确网络配置和权限。
- ❑ 满足内部容器镜像所需的依赖项要求。
- ❑ 目标集群和复制存储库有足够的存储空间。

第 7 章 网络注意事项

检查迁移后用于重定向应用程序网络流量的策略。

7.1. DNS 注意事项

目标集群的 DNS 域与源集群的域不同。默认情况下，应用程序在迁移后获取目标集群的 FQDN。

要保留迁移的应用程序的源 DNS 域，请选择下面描述的两个选项之一。

7.1.1. 将目标集群的 DNS 域与客户端隔离

您可以允许发送到源集群的 DNS 域的客户端请求访问目标集群的 DNS 域，而无需将目标集群公开给客户端。

流程

1. 将外部网络组件（如应用程序负载均衡器或反向代理）放在客户端和目标集群之间。
2. 更新 DNS 服务器上的源集群中的应用程序 FQDN，以返回 exterior 网络组件的 IP 地址。
3. 配置网络组件，将源域中为应用接收的请求发送到目标集群域中的负载均衡器。
4. 为 ***.apps.source.example.com** 域创建一个通配符 DNS 记录，指向源集群的负载均衡器的 IP 地址。
5. 为每个应用程序创建一个 DNS 记录，指向目标集群前面的 exterior 网络组件的 IP 地址。特定的 DNS 记录的优先级高于通配符记录，因此在解决应用 FQDN 时不会发生冲突。

注意

- 外部网络组件必须终止所有安全的 TLS 连接。如果连接传递给目标集群负载均衡器，目标应用程序的 FQDN 会公开给客户端，证书发生错误。
- 应用程序不得将引用目标集群域的链接返回给客户端。否则，应用的某些部分可能无法加载或正常工作。

7.1.2. 设置目标集群以接受源 DNS 域

您可以设置目标集群，以接受源集群的 DNS 域中迁移的应用程序的请求。

流程

对于非安全 HTTP 访问和安全 HTTPS 访问，请执行以下步骤：

1. 在目标集群的项目中创建一个路由，该路由配置为接受源集群中处理的应用程序 FQDN 的请求：

```
$ oc expose svc <app1-svc> --hostname <app1.apps.source.example.com> \
 -n <app1-namespace>
```

新路由就位后，服务器接受对该 FQDN 的任何请求，并将它发送到对应的应用容器集。另外，当迁移应用程序时，会在目标集群域中创建另一个路由。请求会使用这些主机名之一到达迁移的应用。

2. 使用您的 DNS 供应商创建 DNS 记录，将源集群中的应用的 FQDN 指向目标集群的默认负载均衡器的 IP 地址。这会将来自源集群的流量重定向到目标集群。
   应用程序的 FQDN 解析到目标集群的负载均衡器。默认入口控制器路由器接受对该 FQDN 的请求，因为公开了该主机名的路由。

对于安全 HTTPS 访问，请执行以下步骤：

1. 将在安装过程中创建的默认入口控制器的 x509 证书替换为自定义证书。
2. 将这个证书配置为在 **subjectAltName** 字段中为源和目标集群包含通配符 DNS 域。
   新证书对于保护使用 DNS 域进行的连接有效。

其他资源

- 如需更多信息，请参阅替换默认入口证书。

7.2. 网络流量重定向策略

迁移成功后，您必须将无状态应用的网络流量从源集群重定向到目标集群。

重定向网络流量的策略基于以下假设：

- 应用程序 pod 在源集群和目标集群上运行。
- 每个应用都有一个包含源集群主机名的路由。
- 源集群主机名的路由包含 CA 证书。
- 对于 HTTPS，目标路由器 CA 证书包含用于源集群的通配符 DNS 记录的 Subject 备用名称。

考虑以下策略并选择符合您目标的策略。

- 同时重定向所有应用的所有网络流量
  更改源集群的通配符 DNS 记录，使其指向目标集群路由器的虚拟 IP 地址 (VIP)。

  此策略适用于简单应用程序或小型环境的迁移。

- 为单个应用重定向网络流量
  使用指向目标集群路由器 VIP 的源集群主机名为每个应用程序创建一个 DNS 记录。这个 DNS 记录优先于源集群通配符 DNS 记录。

- 为单个应用逐步重定向网络流量

  1. 创建一个代理，用于将流量定向到每个应用程序的源集群路由器的 VIP 和目标集群路由器的 VIP。
  2. 使用指向代理的源集群主机名为每个应用程序创建一个 DNS 记录。
  3. 配置应用的代理条目，将流量百分比路由到目标集群路由器的 VIP，并将其余流量路由到源集群路由器的 VIP。
  4. 逐渐增加您路由到目标集群路由器 VIP 的流量百分比，直到所有网络流量被重定向为止。

- 基于用户的单个应用程序流量重定向
  使用此策略，您可以过滤用户请求的 TCP/IP 标头，以便为预定义的用户组重定向网络流量。这允许您在重定向整个网络流量之前测试用户特定版本的重定向过程。

1. 创建一个代理，用于将流量定向到每个应用程序的源集群路由器的 VIP 和目标集群路由器的 VIP。

2. 使用指向代理的源集群主机名为每个应用程序创建一个 DNS 记录。

3. 配置应用的代理条目，将匹配给定标头模式的流量（如 **测试客户** ）路由到目标集群路由器的 VIP，并将其余流量路由到源集群路由器的 VIP。

4. 将流量分阶段重定向到目标集群路由器的 VIP，直到所有流量都位于目标集群路由器的 VIP 上。

第 8 章 直接迁移要求

Migration Toolkit for Containers (MTC) 1.4.0 或更高版本提供直接迁移。

直接迁移有两个部分：

- 直接卷迁移
- 直接镜像迁移

直接迁移启用持久性卷和内部镜像直接从源集群迁移到目标集群，而无需中间的复制存储库（对象存储）。

8.1. 先决条件

- 为外部流量迁移涉及的集群（源和目标）公开内部 registry。
- 确保远程源和目标集群可以使用端口 443 上的 OpenShift Container Platform 路由进行通信。
- 在源和目标集群集群中配置公开的 registry 路由；通过指定 **spec.exposedRegistryPath** 字段或从 MTC UI 完成此操作。

注意

  - 如果目标集群与主机集群（迁移控制器存在）相同，则不需要为该特定 MTC 集群配置公开的 registry 路由。
  - **spec.exposedRegistryPath** 只适用于直接镜像迁移，而不是直接卷迁移。

- 确保 **MigPlan** 自定义资源 (CR) **indirectImageMigration** 和 **indirectVolumeMigration** 中的两个 spec 标志被设置为 **false**，以便直接执行 Migration。这些标志的默认值为 **false**。

MTC 的直接迁移功能使用 Rsync 工具。

8.2. 用于直接卷迁移的 RSYNC 配置

MTC 中的直接卷迁移 (DVM) 使用 Rsync 在源和目标持久性卷 (PV) 间同步文件，使用两个 PV 之间的直接连接。

rsync 是一个命令行工具，允许您将文件和目录传送到本地和远程目的地。

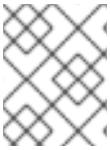
DVM 使用的 **rsync** 命令针对按预期工作的集群进行了优化。

MigrationController CR 会公开以下变量，以便在直接卷迁移中配置 **rsync_options** ：

变量	类型	默认值	描述
rsync_opt_bwlimit	int	未设置	当设置为一个正整数时，**--bwlimit=<int>** 选项被添加到 Rsync 命令中。
rsync_opt_archive	bool	**true**	在 Rsync 命令中设置 **--archive** 选项。

变量	类型	默认值	描述
rsync_opt_partial	bool	**true**	在 Rsync 命令中设置 **--partial** 选项。
rsync_opt_delete	bool	**true**	在 Rsync 命令中设置 **--delete** 选项。
rsync_opt_hardlinks	bool	**true**	设置 **--hard-links** 选项是 Rsync 命令。
rsync_opt_info	string	**COPY2** **DEL2** **REMOVE2** **SKIP2** **FLIST2** **PROGRESS2** **STATS2**	在 Rsync Pod 中启用详细的日志记录。
rsync_opt_extras	string	空	为任何其他任意选项保留。

- 对于所有迁移，通过上述变量设置选项是 *全局的*。当 Operator 成功协调 **MigrationController** CR 时，配置会对将来的所有迁移生效。任何持续迁移都可以使用更新的设置，具体取决于它当前所处的步骤。因此，建议在运行迁移前应用设置。用户始终可以根据需要更新设置。
- 请谨慎使用 **rsync_opt_extras** 变量。使用此变量传递的任何选项都会附加到 **rsync** 命令中，并增加。请确定在指定多个选项时添加空格。指定选项时出现任何错误都可能导致迁移失败。但是，您可以尽可能更新 **MigrationController** CR 以供将来的迁移使用。
- 自定义 **rsync_opt_info** 标志可能会对 MTC 的进度报告功能造成负面影响。但是，删除进度报告可能会具有性能优势。只有在观察到 Rsync 操作的性能无法接受时才应使用这个选项。



注意

DVM 使用的默认配置在各种环境中测试。只要集群健康且运行良好，大多数生产环境用例都可以接受。当默认设置无法正常工作且 Rsync 操作失败时，应使用这些配置变量。

8.2.1. Rsync pod 的资源限制配置

MigrationController CR 会公开以下变量，以便在 Rsync 上配置资源使用量要求和限制：

变量	类型	Default（默认）	描述
source_rsync_pod_cpu_limits	string	**1**	源 rsync pod 的 CPU 限制
source_rsync_pod_memory_limits	string	**1Gi**	源 rsync pod 的内存限值
source_rsync_pod_cpu_requests	string	**400m**	源 rsync pod 的 cpu 请求
source_rsync_pod_memory_requests	string	**1Gi**	源 rsync pod 的内存请求
target_rsync_pod_cpu_limits	string	**1**	目标 rsync pod 的 cpu 限制
target_rsync_pod_cpu_requests	string	**400m**	目标 rsync pod 的 cpu 请求
target_rsync_pod_memory_limits	string	**1Gi**	目标 rsync pod 的内存限值
target_rsync_pod_memory_requests	string	**1Gi**	目标 rsync pod 的内存请求

8.2.1.1. Rsync pod 的补充组配置

如果 PVC 使用共享存储，可以通过将补充组添加到 Rsync pod 定义来配置对存储的访问，以便 pod 允许访问：

变量	类型	Default（默认）	描述
src_supplemental_groups	string	未设置	用于源 Rsync pod 的以逗号分隔的补充组列表
target_supplemental_groups	string	未设置	目标 Rsync pod 的，以逗号分隔的补充组列表

例如，可以更新 **MigrationController** CR 来设置前面的值：

```
spec:
  src_supplemental_groups: "1000,2000"
  target_supplemental_groups: "2000,3000"
```

8.2.1.2. rsync 重试配置

在 MTC 1.4.3 及更新的版本中，引入了重试失败的 Rsync 操作的功能。

默认情况下，迁移控制器会重试 Rsync，直到所有数据都成功从源传输至目标卷或指定重试次数为止。默认重试限制设置为 **20**。

对于较大的卷，限制为 **20** 次重试可能不足。

您可以使用 **MigrationController** CR 中的以下变量增加重试限制：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  rsync_backoff_limit: 40
```

在本例中，重试限制增加到 **40**。

8.2.1.3. 以 root 或非 root 身份运行 Rsync

OpenShift Container Platform 环境默认启用 **PodSecurityAdmission** 控制器。此控制器要求集群管理员通过命名空间标签强制实施 Pod 安全标准。集群中的所有工作负载都应该运行以下 Pod 安全标准级别之一： **Privileged**、**Baseline** 或 **Restricted**。每个集群都有自己的默认策略集。

为了保证在所有环境中成功进行数据传输，MTC 1.7.5 引入了 Rsync pod 中的更改，包括默认以非 root 用户身份运行 Rsync pod。这样可确保即使不一定需要更高特权的工作负载也可以进行数据传输。这个更改是进行的，因为它最适合运行具有最低级别权限的工作负载。

8.2.1.3.1. 为数据 trannsfer 手动覆盖默认非 root 操作

虽然在大多数情况下，以非 root 用户身份运行 Rsync pod 可以正常工作，但当您以 root 用户身份在源端运行工作负载时，数据传输可能会失败。MTC 提供了为数据传输手动覆盖默认非 root 操作的方法：

- 将所有迁移配置为作为 root 在目标集群上针对所有迁移运行 Rsync pod。
- 对于每个迁移，在目标集群上以 root 用户身份运行 Rsync pod。

在这两种情况下，您必须在迁移前运行具有较高特权的工作负载的命名空间源上设置以下标签：**enforce**、**audit** 和 **warn**。

要了解更多有关标签的 Pod Security Admission 和设置值的信息，请参阅 控制 pod 安全准入同步。

8.2.1.3.2. 将所有迁移的 MigrationController CR 配置为 root 或非 root

默认情况下，Rsync 作为非 root 运行。

在目标集群中，您可以将 **MigrationController** CR 配置为以 root 用户身份运行 Rsync。

流程

- 配置 **MigrationController** CR，如下所示：
  -

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  migration_rsync_privileged: true
```

此配置将适用于所有将来的迁移。

8.2.1.3.3. 将 MigMigration CR 配置为每个迁移的根或非 root

在目标集群中，您可以使用以下非 root 选项将 **MigMigration** CR 配置为以 root 或非 root 身份运行 Rsync：

- 作为特定用户 ID (UID)
- 作为一个特定组 ID (GID)

流程

1. 要以 root 用户身份运行 Rsync，请根据本例配置 **MigMigration** CR：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  runAsRoot: true
```

2. 要将 Rsync 作为特定用户 ID (UID)或特定组 ID (GID)运行，请根据本例配置 **MigMigration** CR：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  runAsUser: 10010001
  runAsGroup: 3
```

8.2.2. MigCluster 配置

对于 MTC 中创建的每个 **MigCluster** 资源，在集群中的 Migration Operator 命名空间中创建一个名为 **migration-cluster-config** 的 **ConfigMap**，其中 MigCluster 资源代表。

migration-cluster-config 允许您配置 MigCluster 特定值。Migration Operator 管理 **migration-cluster-config**。

您可以使用 **MigrationController** CR 中公开的变量配置 **ConfigMap** 中的每个值：

变量	类型	必填	描述
migration_stage_image_fqin	string	否	用于 Stage Pod 的镜像（仅适用于 IndirectVolumeMigration）
migration_registry_image_fqin	string	否	用于 Migration Registry 的镜像
rsync_endpoint_type	string	否	数据传输的端点类型（**Route**, **ClusterIP**, **NodePort**）
rsync_transfer_image_fqin	string	否	用于 Rsync Pod 的镜像（仅适用于 DirectVolumeMigration）
migration_rsync_privileged	bool	否	是否以特权方式运行 Rsync Pod
migration_rsync_super_privileged	bool	否	是否将 Rsync Pod 作为超级特权容器运行 (**spc_t** SELinux 上下文)
cluster_subdomain	string	否	集群的子域
migration_registry_readiness_timeout	int	否	Migration Registry 部署的就绪度超时（以秒为单位）
migration_registry_liveness_timeout	int	否	Migration Registry 部署的存活度超时（以秒为单位）
exposed_registry_validation_path	string	否	在 MigCluster 中验证公开的 registry 的子目录 （如 /v2）

8.3. 直接迁移的已知问题

8.3.1. 使用 spc_t 在 OpenShift Container Platform 上运行的工作负载自动应用 Skip SELinux 重新标记临时解决方案

当尝试使用 Migration Toolkit for Containers (MTC)迁移命名空间以及与之关联的大量卷时，**rsync-server** 可能会冻结，且没有提供用于进一步排除此问题的信息。

8.3.1.1. 诊断 Skip SELinux 重新标记临时解决方案

在 kubelet 日志中搜索 **Unable to attach or mount volumes for pod…timed out waiting for the condition** 错误，它来自为 Direct Volume Migration (DVM) 运行 **rsync-server** 的节点。

kubelet 日志示例

```
kubenswrapper[3879]: W0326 16:30:36.749224    3879 volume_linux.go:49] Setting volume ownership for /var/lib/kubelet/pods/8905d88e-6531-4d65-9c2a-eff11dc7eb29/volumes/kubernetes.io~csi/pvc-287d1988-3fd9-4517-a0c7-22539acd31e6/mount and
```

```
fsGroup set. If the volume has a lot of files then setting volume ownership could be slow, see
https://github.com/kubernetes/kubernetes/issues/69699

kubenswrapper[3879]: E0326 16:32:02.706363    3879 kubelet.go:1841] "Unable to attach or mount
volumes for pod; skipping pod" err="unmounted volumes=[8db9d5b032dab17d4ea9495af12e085a],
unattached volumes=[crane2-rsync-server-secret 8db9d5b032dab17d4ea9495af12e085a kube-api-
access-dlbd2 crane2-stunnel-server-config crane2-stunnel-server-secret crane2-rsync-server-config]:
timed out waiting for the condition" pod="caboodle-preprod/rsync-server"

kubenswrapper[3879]: E0326 16:32:02.706496    3879 pod_workers.go:965] "Error syncing pod,
skipping" err="unmounted volumes=[8db9d5b032dab17d4ea9495af12e085a], unattached volumes=
[crane2-rsync-server-secret 8db9d5b032dab17d4ea9495af12e085a kube-api-access-dlbd2 crane2-
stunnel-server-config crane2-stunnel-server-secret crane2-rsync-server-config]: timed out waiting for
the condition" pod="caboodle-preprod/rsync-server" podUID=8905d88e-6531-4d65-9c2a-
eff11dc7eb29
```

8.3.1.2. 使用 Skip SELinux 重新标记临时解决方案解决

要解决这个问题，使用 **MigrationController** 自定义资源(CR)在源和目标 **MigClusters** 中将 **migration_rsync_super_privileged** 参数设置为 **true**。

MigrationController CR 示例

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  migration_rsync_super_privileged: true (1)
  azure_resource_group: ""
  cluster_name: host
  mig_namespace_limit: "10"
  mig_pod_limit: "100"
  mig_pv_limit: "100"
  migration_controller: true
  migration_log_reader: true
  migration_ui: true
  migration_velero: true
  olm_managed: true
  restic_timeout: 1h
  version: 1.8.3
```

(1) **migration_rsync_super_privileged** 参数的值指示是否将 Rsync Pod 作为 *超级特权容器* 运行（**spc_t selinux context**）。有效设置为 **true** 或 **false**。

第 9 章 迁移应用程序

您可以使用 Migration Toolkit for Containers（MTC）web 控制台或命令行来迁移应用程序。

大多数集群范围的资源还没有由 MTC 处理。如果应用程序需要集群范围的资源，则可能需要在目标集群上手动创建。

您可以使用阶段迁移和剪切迁移在集群间迁移应用程序：

- 阶段迁移 (Stage migration) 会在不停止应用程序的情况下将数据从源集群复制到目标集群。您可以多次运行一个阶段迁移来缩短迁移的持续时间。
- 剪切迁移 (Cutover migration) 将停止源集群中的事务，并将资源移到目标集群。

您可以使用状态迁移来迁移应用程序的状态：

- 状态迁移复制所选持久性卷声明 (PVC)。
- 您可以使用状态迁移来迁移同一集群中的命名空间。

在迁移过程中，MTC 会保留以下命名空间注解：

- **openshift.io/sa.scc.mcs**
- **openshift.io/sa.scc.supplemental-groups**
- **openshift.io/sa.scc.uid-range**
  这些注解会保留 UID 范围，确保容器在目标集群中保留其文件系统权限。这可能会存在一定的风险。因为迁移的 UID 可能已存在于目标集群的现有或将来的命名空间中。

9.1. 迁移先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。

直接镜像迁移

- 您必须确保源集群的安全 OpenShift 镜像 registry 已公开。
- 您必须创建指向公开 registry 的路由。

直接卷迁移

- 如果您的集群使用代理，您必须配置 Stunnel TCP 代理。

集群

- 源集群必须升级到最新的 MTC z-stream 版本。
- 在所有集群中，MTC 版本必须相同。

网络

- 集群在相互间有无限制的网络访问，并可以访问复制存储库。
- 如果您复制有 **移动** 的持久性卷，集群必须具有对远程卷的不受限制的网络访问权限。

- 您必须在 OpenShift Container Platform 4 集群中启用以下端口：
  - **6443**（API 服务器）
  - **443**（路由）
  - **53** (DNS)
- 如果使用 TLS，则必须在复制存储库中启用端口 **443**。

持久性卷（PV）

- PV 必须有效。
- PV 必须绑定到持久性卷声明。
- 如果使用快照复制 PV，则需要满足以下额外先决条件：
  - 云供应商必须支持快照。
  - PV 必须具有相同的云供应商。
  - PV 必须位于同一区域。
  - PV 必须具有相同的存储类。

9.2. 使用 MTC WEB 控制台迁移应用程序

您可以使用 MTC web 控制台配置集群和复制存储库。然后，您可以创建并运行迁移计划。

9.2.1. 启动 MTC web 控制台

您可以在浏览器中启动 MTC web 控制台。

先决条件

- MTC web 控制台必须具有到 OpenShift Container Platform Web 控制台的网络访问权限。
- MTC web 控制台必须具有到 OAuth 授权服务器的网络访问权限。

流程

1. 登录到已安装 MTC 的 OpenShift Container Platform 集群。
2. 输入以下命令来获取 MTC web 控制台 URL:

```
$ oc get -n openshift-migration route/migration -o go-template='https://{{ .spec.host }}'
```

   输出类似于以下： **https://migration-openshift-migration.apps.cluster.openshift.com**。
3. 启动浏览器并进入 MTC web 控制台。

注意

如果在安装 MTC 工具套件 Operator 后尝试立即访问 MTC web 控制台，则该控制台可能无法加载，因为 Operator 仍然在配置集群。等待几分钟后重试。

4. 如果您使用自签名的 CA 证书，则会提示您接受源集群 API 服务器的 CA 证书。网页会引导您接受剩余证书的过程。
5. 使用 OpenShift Container Platform 的**用户名**和**密码**进行登陆。

9.2.2. 在 MTC web 控制台中添加集群

您可以在 MTC web 控制台中添加一个集群到 Migration Toolkit for Containers（MTC）web 控制台。

先决条件

- 必须在源集群中配置跨原始资源共享。
- 如果要使用 Azure 快照复制数据：
  - 您必须为集群指定 Azure 资源组名称。
  - 集群必须位于同一 Azure 资源组中。
  - 集群必须位于同一地理位置。
- 如果使用直接镜像迁移，则必须公开到源集群的镜像 registry 的路由。

流程

1. 登录到集群。
2. 获取 **migration-controller** 服务帐户令牌：

```
$ oc create token migration-controller -n openshift-migration
```

输**出示例**

```
eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwi
a3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJtaWciLCJrdWJlcm5ldGVz
LmlvL3NlcnZpY2VhY2NvdW50L3NlY3JldC5uYW1lIjoibWlnLXRva2VuLWs4dDJyIiwia3ViZXJuZ
XRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZXJ2aWNlLWFjY291bnQubmFtZSI6Im1pZyIsImt1YmV
ybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50LnVpZCI6ImE1YjFiYWM
wLWMxYmYtMTFlOS05Y2NiLTAyOWRmODYwYjMwOCIsInN1YiI6InN5c3RlbTpzZXJ2aWNlY
WNjb3VudDptaWc6bWlnIn0.xqeeAINK7UXpdRqAtOj70qhBJPeMwmgLomV9iFxr5RoqUgKchZ
RG2J2rkqmPm6vr7K-
cm7ibD1IBpdQJCcVDuoHYsFgV4mp9vgOfn9osSDp2TGikwNz4Az95e81xnjVUmzh-
NjDsEpw71DH92iHV_xt2sTwtzftS49LpPW2LjrV0evtNBP_t_RfskdArt5VSv25eORl7zScqfe1CiM
kcVbf2UqACQjo3LbkpfN26HAioO2oH0ECPiRzT0Xyh-KwFutJLS9Xgghyw-
LD9kPKcE_xbbJ9Y4Rqajh7WdPYuB0Jd9DPVrslmzK-F6cgHHYoZEv0SvLQi-
PO0rpDrcjOEQQ
```

3. 登录到 MTC web 控制台。
4. 在 MTC web 控制台中点 **Clusters**。

5. 点 **Add cluster**。
6. 填写以下字段：
   - **Cluster name**：集群名称可包含小写字母（**a-z**）和数字（**0-9**）。它不能包含空格或国际字符。
   - **URL**：指定 API 服务器 URL，例如 **https://<www.example.com>:8443**。
   - **Service account token**：粘贴 **migration-controller** 服务帐户令牌。
   - **公开的路由主机到镜像 registry**：如果您使用直接镜像迁移，请指定源集群镜像 registry 公开的路由。
     要创建路由，请运行以下命令：
     - 对于 OpenShift Container Platform 3：

       ```
       $ oc create route passthrough --service=docker-registry --port=5000 -n default
       ```

     - 对于 OpenShift Container Platform 4：

       ```
       $ oc create route passthrough --service=image-registry --port=5000 -n openshift-image-registry
       ```

   - **Azure cluster**：如果使用 Azure 快照复制数据，您必须选择此选项。
     - **Azure resource group**：如果选择了 **Azure cluster**，则会显示此字段。指定 Azure 资源组。
       当在 Microsoft Azure 上创建 OpenShift Container Platform 集群时，会创建一个 Azure Resource Group，使其包含与集群关联的所有资源。在 Azure CLI 中，您可以通过发出以下命令显示所有资源组：

       ```
       $ az group list
       ```

       与 OpenShift Container Platform 集群关联的 **ResourceGroups** 被标记，其中 **sample-rg-name** 是您要提取并提供给 UI 的值：

       ```
       {
         "id": "/subscriptions/...//resourceGroups/sample-rg-name",
         "location": "centralus",
         "name": "...",
         "properties": {
           "provisioningState": "Succeeded"
         },
         "tags": {
           "kubernetes.io_cluster.sample-ld57c": "owned",
           "openshift_creationDate": "2019-10-25T23:28:57.988208+00:00"
         },
         "type": "Microsoft.Resources/resourceGroups"
       },
       ```

       此信息也可从 **资源组** 刀片的 Azure 门户 获取。
   - **需要 SSL 验证** ：可选：选择这个选项来验证到集群的安全套接字层(SSL)连接。

- **CA bundle file**：如果选择了 **Require SSL 验证**，则会显示此字段。如果您为自签名证书创建了自定义 CA 证书捆绑包文件，请点 **Browse**，选择 CA 捆绑包文件并上传它。

7. 点 **Add cluster**。
   集群会出现在 **Clusters** 列表中。

9.2.3. 在 MTC web 控制台中添加复制存储库

您可以将对象存储作为复制存储库添加到 MTC web 控制台的 Migration Toolkit for Containers (MTC) web 控制台中。

MTC 支持以下存储供应商：

- Amazon Web Services (AWS) S3
- 多云对象网关 (MCG)
- 通用 S3 对象存储，例如 Minio 或 Ceph S3
- Google Cloud Provider (GCP)
- Microsoft Azure Blob

先决条件

- 您必须将对象存储配置为复制存储库。

流程

1. 在 MTC web 控制台中点 **Replication repositories**。
2. 点 **Add repository**。
3. 选择 **Storage provider type** 并填写以下字段：
   - 用于 S3 供应商的 **AWS**，包括 AWS 和 MCG:
     - **Replication repository name**：指定 MTC web 控制台中的复制存储库。
     - **S3 bucket name**：指定 S3 存储桶的名称。
     - **S3 bucket region**：指定 S3 存储桶区域。AWS S3 **必填**。对于某些 S3 供应商是**可选的**。检查 S3 供应商的产品文档，以获取预期值。
     - **S3 端点**：指定 S3 服务的 URL，而不是存储桶，例如：**https://<s3-storage.apps.cluster.com>**。通用 S3 供应商**必填**。您必须使用 **https://** 前缀。
     - **S3 provider access key**：为 AWS 指定 **<AWS_SECRET_ACCESS_KEY>**，或者为 MCG 和其他 S3 供应商指定 S3 供应商访问密钥。
     - **S3 provider secret access key**：为 AWS 指定 **<AWS_ACCESS_KEY_ID>**，或为 MCG 和其他 S3 供应商指定 S3 provider secret 访问密钥。
     - **Require SSL verification**：如果您使用的是通用 S3 供应商，则清除此复选框。
     - 如果您为自签名证书创建了自定义 CA 证书捆绑包，点 **Browse** 并浏览到 Base64 编码的文件。

- GCP：
  - **Replication repository name**：指定 MTC web 控制台中的复制存储库。
  - **GCP bucket name**：指定 GCP 存储桶的名称。
  - **GCP credential JSON blob**：在 **credentials-velero** 文件中指定字符串。
- Azure：
  - **Replication repository name**：指定 MTC web 控制台中的复制存储库。
  - **Azure resource group**：指定 Azure Blob 存储的资源组。
  - **Azure storage account name**：指定 Azure Blob 存储帐户名称。
  - **Azure credentials - INI file contents**：在 **credentials-velero** 文件中指定字符串。

4. 点 **Add repository** 并等待连接验证。
5. 点 **Close**。
   新仓库会出现在 **Replication repositories** 列表中。

9.2.4. 在 MTC web 控制台中创建迁移计划

您可以在 Migration Toolkit for Containers（MTC）web 控制台中创建一个迁移计划。

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。
- 您必须确保在所有集群中安装相同的 MTC 版本。
- 您必须在 MTC web 控制台中添加集群和复制存储库。
- 如果要使用 *move* 数据复制方法迁移持久性卷（PV），则源和目标集群必须有对远程卷的不间断网络访问权限。
- 如果要使用直接镜像迁移，您必须指定源集群的镜像 registry 公开的路由。这可以通过使用 MTC web 控制台或更新 **MigCluster** 自定义资源清单来实现。

流程

1. 在 MTC web 控制台中点 **Migration Plan**。
2. 点 **Add migration plan**。
3. 输入 **Plan 名称**。
   迁移计划名称不能超过 253 个小写字母数字字符（**a-z, 0-9**），且不能包含空格或下划线（_）。
4. 选择 **Source cluster**、**Target cluster** 和 **Repository**。
5. 点击 **Next**。
6. 选择要迁移的项目。
7. 可选：点击项目旁边的编辑图标来更改目标命名空间。

8. 点击 **Next**。

9. 为每个 PV 选择一个 **迁移类型**：

   - **Copy** 选项将源集群的 PV 中的数据复制到复制存储库中，然后在目标集群中恢复新创建的具有类似特征的 PV 上的数据。

   - **Move** 选项从源集群中卸载一个远程卷（例如 NFS），在目标集群上创建一个指向这个远程卷的 PV 资源，然后在目标集群中挂载远程卷。在目标集群中运行的应用程序使用源集群使用的同一远程卷。

10. 点击 **Next**。

11. 为每个 PV 选择 **Copy method**：

    - **快照复制**使用云供应商的快照功能备份和恢复数据。它比 **Filesystem copy** 要快得多。

    - **Filesystem copy** 备份源集群中的文件，并在目标集群中恢复它们。
      直接卷迁移需要使用文件系统复制方法。

12. 您可以选择 **Verify copy** 来验证使用 **Filesystem copy** 迁移的数据。数据是通过为每个源文件生成 checksum 并在恢复后检查 checksum 来验证。数据校验可能会显著降低性能。

13. 选择 **目标存储类**。
    如果选择了 **Filesystem copy**，您可以更改目标存储类。

14. 点击 **Next**。

15. 在 **Migration options** 页面上，如果您为源集群指定了公开的镜像 registry 路由，则会选择 **Direct 镜像迁移** 选项。如果使用 **Filesystem copy** 迁移数据，**Direct PV migration** 选项会被选择。
    直接迁移选项将镜像和文件直接从源集群复制到目标集群。这个选项比将源集群的镜像和文件复制到复制存储库，然后再从复制存储库复制到目标集群要快。

16. 点击 **Next**。

17. 可选：点 **Add Hook** 在迁移计划中添加 hook。
    hook 运行自定义代码。您可以在单个迁移计划中最多添加四个 hook。每个 hook 在不同的迁移步骤中运行。

    a. 在 web 控制台中输入要显示的 hook 名称。

    b. 如果 hook 是一个 Ansible playbook，请选择 **Ansible playbook**，然后点 **Browse** 上传 playbook，或在字段中粘贴 playbook 的内容。

    c. 可选： 如果不使用默认 hook 镜像，请指定 Ansible 运行时镜像。

    d. 如果 hook 不是 Ansible playbook，选择 **Custom container image** 并指定镜像名称和路径。
       自定义容器镜像可以包含 Ansible playbook。

    e. 选择 **Source cluster** 或 **Target cluster**。

    f. 输入 **Service account name** 和 **Service account namespace**。

    g. 为 hook 选择迁移步骤：

       - **preBackup**：在应用程序工作负载在源集群中备份前

- **PostBackup**：在应用程序工作负载在源集群中备份后
- **preRestore**：在目标集群中恢复应用程序工作负载前
- **postRestore**：在目标集群中恢复应用程序工作负载后

h. 点击 **Add**。

18. 点 **Finish**。
迁移计划显示在 **Migration Plan** 列表中。

持久性卷复制方法的其他资源

- MTC 文件系统复制方法
- MTC 快照复制方法

9.2.5. 在 MTC web 控制台中运行迁移计划

您可以使用在 Migration Toolkit for Containers（MTC）web 控制台中创建的迁移计划来迁移应用程序和数据。

注意

迁移过程中，在目标集群中，MTC 将迁移的持久性卷（PV）的重新声明策略设置为 **Retain**。

Backup 自定义资源包含一个 **PVOriginalReclaimPolicy** 注解，用于指示原始重新声明策略。您可以手动恢复迁移 PV 的重新声明策略。

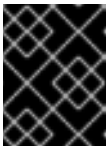
先决条件

MTC web 控制台必须包含以下内容：

- 处于 **Ready** 状态的源集群
- 处于 **Ready** 状态的目标集群
- 复制软件仓库
- 有效的迁移计划

流程

1. 登录到 MTC web 控制台并点 **迁移计划**。
2. 点击迁移计划  旁边的 Options 菜单，并在 **Migration** 中选择以下选项之一：
   - **stage** 在不停止应用程序的情况下将数据从源集群复制到目标集群。
   - **cutover** 会停止源集群上的事务，并将资源移到目标集群。
   可选：在 **Cutover 迁移** 对话框中，您可以清除 **Halt transactions on the source cluster during migration** 多选设置。
   - **State** 会复制所选持久性卷声明(PVC)。



重要

不要使用状态迁移来在集群之间迁移命名空间。使用 stage 或 cutover migration。

- 在**状态迁移**对话框中选择一个或多个 PVC 并点 **Migrate**。

3. 迁移完成后，在 OpenShift Container Platform web 控制台中确认已成功迁移了应用程序：
   a. 点 **Home → Projects**。
   b. 点迁移的项目查看其状态。
   c. 在 **Routes** 部分，点击 **Location** 验证应用程序是否正常运行。
   d. 点 **Workloads → Pods** 来验证 pod 是否在迁移的命名空间中运行。
   e. 点 **Storage → Persistent volumes** 来验证是否正确置备了已迁移的持久性卷。

第 10 章 高级迁移选项

您可以自动化迁移并修改 **MigPlan** 和 **MigrationController** 自定义资源，以执行大规模迁移并提高性能。

10.1. 术语

表 10.1. MTC 术语

术语	定义
源集群	从中迁移应用程序的集群。
目标集群[1]	将应用程序迁移到的集群。
复制软件仓库	用于在间接迁移过程中复制镜像、卷和 Kubernetes 对象的对象存储，或者用于直接卷迁移或直接镜像迁移期间 Kubernetes 对象的对象存储。 复制存储库必须可以被所有集群访问。
主机集群	运行 **migration-controller** pod 和 Web 控制台的集群。主机集群通常是目标集群，但这不是必需的。 主机集群不需要公开的 registry 路由来直接迁移镜像。
远程集群	远程集群通常是源集群，但这不是必需的。 远程集群需要一个包含 **migration-controller** 服务帐户令牌的 **Secret** 自定义资源。 远程集群需要一个公开的安全 registry 路由来直接迁移镜像。
间接迁移	镜像、卷和 Kubernetes 对象从源集群复制到复制存储库，然后从复制存储库复制到目标集群。
直接卷迁移	持久性卷直接从源集群复制到目标集群。
直接镜像迁移	镜像直接从源集群复制到目标集群。
阶段迁移	在不停止应用程序的情况下，数据将复制到目标集群。 多次运行阶段迁移会缩短迁移的持续时间。
剪切迁移	应用在源集群中停止，其资源迁移到目标集群。
状态迁移	通过将特定的持久性卷声明复制到目标集群来迁移应用程序状态。
回滚迁移	回滚迁移会回滚一个已完成的迁移。

[1] 在 MTC web 控制台中称为 *目标集群*。

10.2. 使用命令行迁移应用程序

您可以使用命令行界面 (CLI) 使用 MTC API 迁移应用程序，以便自动执行迁移。

10.2.1. 迁移先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。

直接镜像迁移

- 您必须确保源集群的安全 OpenShift 镜像 registry 已公开。
- 您必须创建指向公开 registry 的路由。

直接卷迁移

- 如果您的集群使用代理，您必须配置 Stunnel TCP 代理。

集群

- 源集群必须升级到最新的 MTC z-stream 版本。
- 在所有集群中，MTC 版本必须相同。

网络

- 集群在相互间有无限制的网络访问，并可以访问复制存储库。
- 如果您复制有 **移动** 的持久性卷，集群必须具有对远程卷的不受限制的网络访问权限。
- 您必须在 OpenShift Container Platform 4 集群中启用以下端口：
  - **6443**（API 服务器）
  - **443**（路由）
  - **53** (DNS)
- 如果使用 TLS，则必须在复制存储库中启用端口 **443**。

持久性卷（PV）

- PV 必须有效。
- PV 必须绑定到持久性卷声明。
- 如果使用快照复制 PV，则需要满足以下额外先决条件：
  - 云供应商必须支持快照。
  - PV 必须具有相同的云供应商。
  - PV 必须位于同一区域。
  - PV 必须具有相同的存储类。

10.2.2. 创建用于直接镜像迁移的 registry 路由

要直接镜像迁移，您必须在所有远程集群中创建指向公开的 OpenShift 镜像 registry 的路由。

先决条件

- OpenShift 镜像 registry 必须公开给所有远程集群上的外部流量。
  OpenShift Container Platform 4 registry 默认公开。

流程

- 要创建到 OpenShift Container Platform 4 registry 的路由，请运行以下命令：

```
$ oc create route passthrough --service=image-registry -n openshift-image-registry
```

10.2.3. 代理配置

对于 OpenShift Container Platform 4.1 及更早的版本，您必须在安装 Migration Toolkit for Containers Operator 后，在 **MigrationController** 自定义资源 (CR) 清单中配置代理，因为这些版本不支持集群范围的 **proxy** 对象。

对于 OpenShift Container Platform 4.2 到 4.15，Migration Toolkit for Containers (MTC) 会继承集群范围的代理设置。如果要覆盖集群范围的代理设置，可以更改代理参数。

10.2.3.1. 直接卷迁移

MTC 1.4.2 中引入了直接卷迁移(DVM)。DVM 只支持一个代理。如果目标集群也位于代理后面，则源集群无法访问目标集群的路由。

如果要从代理后面的源集群执行 DVM，您必须配置一个 TCP 代理，该代理可在传输层进行透明处理，并在不使用自己的 SSL 证书的情况下转发 SSL 连接。Stunnel 代理是此类代理的示例。

10.2.3.1.1. DVM 的 TCP 代理设置

您可以通过 TCP 代理在源和目标集群之间设置直接连接，并在 **MigrationController** CR 中配置 **stunnel_tcp_proxy** 变量来使用代理：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  stunnel_tcp_proxy: http://username:password@ip:port
```

直接卷迁移(DVM)只支持代理的基本身份验证。此外，DVM 仅适用于可透明地传输 TCP 连接的代理。在 man-in-the-middle 模式中的 HTTP/HTTPS 代理无法正常工作。现有的集群范围的代理可能不支持此行为。因此，DVM 的代理设置意与 MTC 中常见的代理配置不同。

10.2.3.1.2. 为什么使用 TCP 代理而不是 HTTP/HTTPS 代理？

您可以通过 OpenShift 路由在源和目标集群之间运行 Rsync 来启用 DVM。流量通过 TCP 代理(Stunnel)加密。在源集群上运行的 Stunnel 会启动与目标 Stunnel 的 TLS 连接，并通过加密频道来传输数据。

OpenShift 中的集群范围 HTTP/HTTPS 代理通常在 man-in-the-middle 模式进行配置，其中它们将自己的 TLS 会话与外部服务器协商。但是，这不适用于 Stunnel。Stunnel 要求代理不处理它的 TLS 会话，基本上使代理成为一个透明的隧道，只需按原样转发 TCP 连接。因此，您必须使用 TCP 代理。

10.2.3.1.3. 已知问题

迁移失败并显示 Upgrade request required 错误

迁移控制器使用 SPDY 协议在远程 pod 中执行命令。如果远程集群位于代理或不支持 SPDY 协议的防火墙后，迁移控制器将无法执行远程命令。迁移失败并显示出错信息 **Upgrade request required**。临时解决方案： 使用支持 SPDY 协议的代理。

除了支持 SPDY 协议外，代理或防火墙还必须将 **Upgrade** HTTP 标头传递给 API 服务器。客户端使用此标头打开与 API 服务器的 websocket 连接。如果代理或防火墙阻止 **Upgrade** 标头，则迁移会失败，并显示出错信息 **Upgrade request required**。临时解决方案：确保代理转发 **Upgrade** 标头。

10.2.3.2. 为迁移调优网络策略

OpenShift 支持根据集群使用的网络插件，限制使用 *NetworkPolicy* 或 *EgressFirewalls* 的流量。如果任何涉及迁移的源命名空间使用此类机制将网络流量限制到 pod，限制可能会在迁移过程中停止到 Rsync pod 的流量。

在源和目标集群上运行的 rsync pod 必须通过 OpenShift Route 相互连接。可将现有的 *NetworkPolicy* 或 *EgressNetworkPolicy* 对象配置为从这些流量限制自动排除 Rsync pod。

10.2.3.2.1. NetworkPolicy 配置

10.2.3.2.1.1. 来自 Rsync pod 的出口流量

如果源或目标命名空间中的 **NetworkPolicy** 配置阻止这种类型的流量，您可以使用 Rsync pod 的唯一标签来允许出口流量从它们传递。以下策略允许来自命名空间中 Rsync pod 的**所有**出口流量：

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-from-rsync-pods
spec:
  podSelector:
    matchLabels:
      owner: directvolumemigration
      app: directvolumemigration-rsync-transfer
  egress:
  - {}
  policyTypes:
  - Egress
```

10.2.3.2.1.2. 到 Rsync pod 的入口流量

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-from-rsync-pods
spec:
  podSelector:
```

```
    matchLabels:
      owner: directvolumemigration
      app: directvolumemigration-rsync-transfer
  ingress:
  - {}
  policyTypes:
  - Ingress
```

10.2.3.2.2. EgressNetworkPolicy 配置

EgressNetworkPolicy 对象或 *Egress Firewalls* 是 OpenShift 构造，用于阻止离开集群的出口流量。

与 **NetworkPolicy** 对象不同，egress Firewall 在项目级别工作，因为它适用于命名空间中的所有 pod。因此，Rsync pod 的唯一标签不会使只有 Rsync pod 的 Rsync pod 冲突。但是，您可以将源集群或目标集群的 CIDR 范围添加到策略的 *Allow* 规则中，以便可以在两个集群之间设置直接连接。

根据存在 Egress Firewall 的集群，您可以添加其他集群的 CIDR 范围来允许两者间的出口流量：

```
apiVersion: network.openshift.io/v1
kind: EgressNetworkPolicy
metadata:
  name: test-egress-policy
  namespace: <namespace>
spec:
  egress:
  - to:
      cidrSelector: <cidr_of_source_or_target_cluster>
    type: Deny
```

10.2.3.2.3. 为数据传输选择备用端点

默认情况下，DVM 使用 OpenShift Container Platform 路由作为端点，将 PV 数据传送到目标集群。如果集群拓扑允许，您可以选择其他类型的支持的端点。

对于每个集群，您可以通过在 **MigrationController** CR 中适当的 **目标集群上设置 rsync_endpoint_type** 变量来配置端点：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  [...]
  rsync_endpoint_type: [NodePort|ClusterIP|Route]
```

10.2.3.2.4. 为 Rsync pod 配置补充组

当 PVC 使用共享存储时，您可以通过将 supplemental 组添加到 Rsync pod 定义来配置对存储的访问，以便 pod 允许访问：

表 10.2. Rsync pod 的附加组群

变量	类型	Default（默认）	描述
src_supplemental_groups	string	未设置	用于源 Rsync pod 的以逗号分隔的补充组列表
target_supplemental_groups	string	未设置	目标 Rsync pod 的，以逗号分隔的补充组列表

用法示例

可以更新 **MigrationController** CR，以便为这些补充组设置值：

```
spec:
  src_supplemental_groups: "1000,2000"
  target_supplemental_groups: "2000,3000"
```

10.2.3.3. 配置代理

先决条件

- 必须使用在所有集群中具有 **cluster-admin** 权限的用户登录。

流程

1. 获取 **MigrationController** CR 清单：

```
$ oc get migrationcontroller <migration_controller> -n openshift-migration
```

2. 更新代理参数：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: <migration_controller>
  namespace: openshift-migration
...
spec:
  stunnel_tcp_proxy: http://<username>:<password>@<ip>:<port> 1
  noProxy: example.com 2
```

1. 用于直接卷迁移的 stunnel 代理 URL。
2. 要排除代理的目标域名、域、IP 地址或其他网络 CIDR 的逗号分隔列表。

在域前面加 **.** 来仅匹配子域。例如： **.y.com** 匹配 **x.y.com**，但不匹配 **y.com**。使用 * 可对所有目的地绕过所有代理。如果您扩展了未包含在安装配置中 **networking.machineNetwork[].cidr** 字段定义的 worker，您必须将它们添加到此列表中，以防止连接问题。

如果未设置 **httpProxy** 和 **httpsProxy** 字段，则此字段将被忽略。

3. 将清单保存为 **migration-controller.yaml**。

4. 应用更新的清单：

```
$ oc replace -f migration-controller.yaml -n openshift-migration
```

10.2.4. 使用 MTC API 迁移应用程序

您可以使用 MTC API 从命令行迁移应用程序。

流程

1. 为主机集群创建一个 **MigCluster** CR 清单：

```
$ cat << EOF | oc apply -f -
apiVersion: migration.openshift.io/v1alpha1
kind: MigCluster
metadata:
  name: <host_cluster>
  namespace: openshift-migration
spec:
  isHostCluster: true
EOF
```

2. 为每个远程集群创建一个 **Secret** 对象清单：

```
$ cat << EOF | oc apply -f -
apiVersion: v1
kind: Secret
metadata:
  name: <cluster_secret>
  namespace: openshift-config
type: Opaque
data:
  saToken: <sa_token> (1)
EOF
```

(1) 指定远程集群的 base64 编码的 **migration-controller** 服务帐户（SA）令牌。您可以运行以下命令来获取令牌：

```
$ oc sa get-token migration-controller -n openshift-migration | base64 -w 0
```

3. 为每个远程集群创建一个 **MigCluster** CR 清单：

```
$ cat << EOF | oc apply -f -
apiVersion: migration.openshift.io/v1alpha1
kind: MigCluster
metadata:
  name: <remote_cluster> (1)
  namespace: openshift-migration
spec:
  exposedRegistryPath: <exposed_registry_route> (2)
```

```
  insecure: false 3
  isHostCluster: false
  serviceAccountSecretRef:
    name: <remote_cluster_secret> 4
    namespace: openshift-config
  url: <remote_cluster_url> 5
EOF
```

1. 指定远程集群的 **Cluster** CR。
2. 可选：要直接镜像迁移，请指定公开的 registry 路由。
3. 如果 **false** 则启用 SSL 验证。如果为 **true**，则不需要 CA 证书或不检查 CA 证书。
4. 指定远程集群的 **Secret** 对象。
5. 指定远程集群的 URL。

4. 验证所有集群是否处于 **Ready** 状态：

```
$ oc describe MigCluster <cluster>
```

5. 为复制存储库创建 **Secret** 对象清单：

```
$ cat << EOF | oc apply -f -
apiVersion: v1
kind: Secret
metadata:
  namespace: openshift-config
  name: <migstorage_creds>
type: Opaque
data:
  aws-access-key-id: <key_id_base64> 1
  aws-secret-access-key: <secret_key_base64> 2
EOF
```

1. 指定 base64 格式的密钥 ID。
2. 指定 base64 格式的 secret 密钥。

AWS 凭证默认为 base64 编码。对于其他存储供应商，您必须使用每个密钥运行以下命令来对凭证进行编码：

```
$ echo -n "<key>" | base64 -w 0 1
```

1. 指定密钥 ID 或 secret 密钥。这两个密钥都必须都是 base64 编码。

6. 为复制存储库创建一个 **MigStorage** CR 清单：

```
$ cat << EOF | oc apply -f -
apiVersion: migration.openshift.io/v1alpha1
kind: MigStorage
```

```
metadata:
  name: <migstorage>
  namespace: openshift-migration
spec:
  backupStorageConfig:
    awsBucketName: <bucket> 1
    credsSecretRef:
      name: <storage_secret> 2
      namespace: openshift-config
  backupStorageProvider: <storage_provider> 3
  volumeSnapshotConfig:
    credsSecretRef:
      name: <storage_secret> 4
      namespace: openshift-config
  volumeSnapshotProvider: <storage_provider> 5
EOF
```

1. 指定存储桶名称。
2. 指定对象存储的 **Secrets** CR。您必须确保存储在对象存储的 **Secrets** CR 中的凭证是正确的。
3. 指定存储供应商。
4. 可选：如果要使用快照复制数据，请指定对象存储的 **Secrets** CR。您必须确保存储在对象存储的 **Secrets** CR 中的凭证是正确的。
5. 可选：如果您使用快照复制数据，请指定存储供应商。

7. 验证 **MigStorage** CR 是否处于 **Ready** 状态：

```
$ oc describe migstorage <migstorage>
```

8. 创建一个 **MigPlan** CR 清单：

```
$ cat << EOF | oc apply -f -
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  name: <migplan>
  namespace: openshift-migration
spec:
  destMigClusterRef:
    name: <host_cluster>
    namespace: openshift-migration
  indirectImageMigration: true 1
  indirectVolumeMigration: true 2
  migStorageRef:
    name: <migstorage> 3
    namespace: openshift-migration
  namespaces:
    - <source_namespace_1> 4
    - <source_namespace_2>
    - <source_namespace_3>:<destination_namespace> 5
```

```
  srcMigClusterRef:
    name: <remote_cluster> 6
    namespace: openshift-migration
EOF
```

1. 如果为 **false**，则启用直接镜像迁移。
2. 如果为 **false**，则启用直接卷迁移。
3. 指定 **MigStorage** CR 实例的名称。
4. 指定一个或多个源命名空间。默认情况下，目标命名空间具有相同的名称。
5. 如果目标命名空间与源命名空间不同，请指定目标命名空间。
6. 指定源集群 **MigCluster** 实例的名称。

9. 验证 **MigPlan** 实例是否处于 **Ready** 状态：

```
$ oc describe migplan <migplan> -n openshift-migration
```

10. 创建一个 **MigMigration** CR 清单，以启动 **MigPlan** 实例中定义的迁移：

```
$ cat << EOF | oc apply -f -
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  name: <migmigration>
  namespace: openshift-migration
spec:
  migPlanRef:
    name: <migplan> 1
    namespace: openshift-migration
  quiescePods: true 2
  stage: false 3
  rollback: false 4
EOF
```

1. 指定 **MigPlan** CR 名称。
2. 如果为 **true**，则源集群上的 pod 会在迁移前停止。
3. 如果为 **true**，则进行阶段（stage）迁移，即在不停止应用程序的情况下复制大多数数据。
4. 如果为 **true**，则会回滚到一个已完成的迁移。

11. 通过观察 **MigMigration** CR 进度来验证迁移：

```
$ oc watch migmigration <migmigration> -n openshift-migration
```

输出类似于以下：

输**出示例**

```
Name:         c8b034c0-6567-11eb-9a4f-0bc004db0fbc
Namespace:    openshift-migration
Labels:       migration.openshift.io/migplan-name=django
Annotations:  openshift.io/touch: e99f9083-6567-11eb-8420-0a580a81020c
API Version:  migration.openshift.io/v1alpha1
Kind:         MigMigration
...
Spec:
  Mig Plan Ref:
    Name:       migplan
    Namespace:  openshift-migration
  Stage:        false
Status:
  Conditions:
    Category:              Advisory
    Last Transition Time:  2021-02-02T15:04:09Z
    Message:               Step: 19/47
    Reason:                InitialBackupCreated
    Status:                True
    Type:                  Running
    Category:              Required
    Last Transition Time:  2021-02-02T15:03:19Z
    Message:               The migration is ready.
    Status:                True
    Type:                  Ready
    Category:              Required
    Durable:               true
    Last Transition Time:  2021-02-02T15:04:05Z
    Message:               The migration registries are healthy.
    Status:                True
    Type:                  RegistriesHealthy
  Itinerary:               Final
  Observed Digest:
7fae9d21f15979c71ddc7dd075cb97061895caac5b936d92fae967019ab616d5
  Phase:                   InitialBackupCreated
  Pipeline:
    Completed:  2021-02-02T15:04:07Z
    Message:    Completed
    Name:       Prepare
    Started:    2021-02-02T15:03:18Z
    Message:    Waiting for initial Velero backup to complete.
    Name:       Backup
    Phase:      InitialBackupCreated
    Progress:
      Backup openshift-migration/c8b034c0-6567-11eb-9a4f-0bc004db0fbc-wpc44: 0 out of
estimated total of 0 objects backed up (5s)
    Started:        2021-02-02T15:04:07Z
    Message:        Not started
    Name:           StageBackup
    Message:        Not started
    Name:           StageRestore
    Message:        Not started
    Name:           DirectImage
    Message:        Not started
    Name:           DirectVolume
    Message:        Not started
```

```
  Name:         Restore
  Message:      Not started
  Name:         Cleanup
 Start Timestamp:  2021-02-02T15:03:18Z
Events:
 Type    Reason   Age                From                    Message
 ----    ------   ----               ----                    -------
 Normal  Running  57s                migmigration_controller  Step: 2/47
 Normal  Running  57s                migmigration_controller  Step: 3/47
 Normal  Running  57s (x3 over 57s)   migmigration_controller  Step: 4/47
 Normal  Running  54s                migmigration_controller  Step: 5/47
 Normal  Running  54s                migmigration_controller  Step: 6/47
 Normal  Running  52s (x2 over 53s)   migmigration_controller  Step: 7/47
 Normal  Running  51s (x2 over 51s)   migmigration_controller  Step: 8/47
 Normal  Ready    50s (x12 over 57s)  migmigration_controller  The migration is ready.
 Normal  Running  50s                migmigration_controller  Step: 9/47
 Normal  Running  50s                migmigration_controller  Step: 10/47
```

10.2.5. 状态迁移

您可以使用 Migration Toolkit for Containers(MTC)迁移组成应用程序状态的持久性卷声明(PVC)，执行可重复的、仅状态的迁移。您可以通过从迁移计划中排除其他 PVC 来迁移指定的 PVC。您可以映射 PVC 以确保源和目标 PVC 同步。持久性卷 (PV) 数据复制到目标集群。PV 引用不会被移动，应用程序 pod 将继续在源集群中运行。

State 迁移专门设计用于外部 CD 机制，如 OpenShift Gitops。在使用 MTC 迁移状态时，您可以使用 GitOps 迁移应用程序清单。

如果您有 CI/CD 管道，您可以通过在目标集群中部署无状态组件来迁移它们。然后，您可以使用 MTC 迁移有状态组件。

您可以在集群间或同一集群中执行状态迁移。

重要

状态迁移仅迁移构成应用状态的组件。如果要迁移整个命名空间，请使用 stage 或 cutover migration。

先决条件

- 源集群中的应用程序状态在通过 **PersistentVolumeClaims** 置备的 **PersistentVolume** 中保留。
- 应用程序的清单在中央存储库中可用，它们同时可从源和目标集群访问。

流程

1. 将持久性卷数据从源迁移到目标集群。
   您可以根据需要多次执行此步骤。源应用程序继续运行。
2. 静止源应用程序。
   您可以通过在源集群上直接将工作负载资源副本设置为 **0** 来完成此操作，或者更新 GitHub 中的清单并重新同步 Argo CD 应用程序。
3. 将应用程序清单克隆到目标集群。
   您可以使用 Argo CD 将应用程序清单克隆到目标集群。

4. 将剩余的卷数据从源迁移到目标集群。
   通过执行最终数据迁移，在状态迁移过程中迁移应用程序创建的任何新数据。

5. 如果克隆的应用程序处于静默状态，请取消静止它。

6. 将 DNS 记录切换到目标集群，将用户流量重新定向到已迁移的应用程序。

注意

在执行状态迁移时，MTC 1.6 无法自动静止应用程序。它只能迁移 PV 数据。因此，您必须使用 CD 机制来静止或取消静止应用程序。

MTC 1.7 引入了明确的 Stage 和 Cutover 流。您可以根据需要，使用暂存来执行初始数据传输。然后，您可以执行一个可自动静止源应用程序。

其他资源

- 请参阅将 PVC 从迁移中排除以选择 PVC。
- 请参阅映射 PVC，将源 PV 数据迁移到目标集群上置备的 PVC。
- 请参阅迁移 Kubernetes 对象 以迁移组成应用程序状态的 Kubernetes 对象。

10.3. 迁移 HOOK

您可以在单个迁移计划中添加最多四个迁移 hook，每个 hook 在迁移过程的不同阶段运行。迁移 hook 执行的任务包括自定义应用程序默认、手动迁移不受支持的数据类型以及在迁移后更新应用程序。

迁移 hook 会在以下迁移步骤之一中，在源或目标集群上运行：

- **PreBackup**：在源集群中备份资源前。
- **PostBackup**：在源集群中备份资源后。
- **PreRestore**：在目标集群上恢复资源前。
- **PostRestore**：在目标集群中恢复资源后。

您可以通过创建使用默认 Ansible 镜像运行的 Ansible playbook 或者使用自定义 hook 容器来创建 hook。

Ansible playbook

Ansible playbook 作为一个配置映射挂载到 hook 容器上。hook 容器使用 **MigPlan** 自定义资源中指定的集群、服务帐户和命名空间以作业的形式运行。作业会继续运行，直到达到默认限制的 6 次重试或成功完成为止。即使初始 pod 被驱除或终止，也会继续。

默认 Ansible 运行时镜像为 **registry.redhat.io/rhmtc/openshift-migration-hook-runner-rhel7:1.8**。此镜像基于 Ansible Runner 镜像，并包含 Ansible Kubernetes 资源的 **python-openshift**，以及更新的 **oc** 二进制文件。

自定义 hook 容器

您可以使用自定义 hook 容器而不是默认的 Ansible 镜像。

10.3.1. 为迁移 hook 编写 Ansible playbook

您可以编写 Ansible playbook 以用作迁移 hook。通过使用 MTC web 控制台或在 **MigPlan** 自定义资源（CR）清单中指定 **spec.hooks** 参数的值来在迁移计划中添加 hook。

Ansible playbook 作为一个配置映射挂载到 hook 容器上。hook 容器使用 **MigPlan** CR 中指定的集群、服务帐户和命名空间以作业的形式运行。hook 容器使用指定的服务帐户令牌，以便当任务在集群中运行前无需进行身份验证。

10.3.1.1. Ansible 模块

您可以使用 Ansible **shell** 模块来运行 **oc** 命令。

shell 模块示例

```
- hosts: localhost
  gather_facts: false
  tasks:
  - name: get pod name
    shell: oc get po --all-namespaces
```

您可以使用 **kubernetes.core** 模块（如 **k8s_info** ）与 Kubernetes 资源交互。

k8s_facts 模块示例

```
- hosts: localhost
  gather_facts: false
  tasks:
  - name: Get pod
    k8s_info:
      kind: pods
      api: v1
      namespace: openshift-migration
      name: "{{ lookup( 'env', 'HOSTNAME') }}"
    register: pods

  - name: Print pod name
    debug:
      msg: "{{ pods.resources[0].metadata.name }}"
```

在非零退出状态通常不会生成的情况下，可以使用 **fail** 模块生成一个非零退出状态，以确保可以检测到 hook 的成功或失败。hook 以作业形式运行，hook 的成功或失败状态取决于作业容器的退出状态。

fail 模块示例

```
- hosts: localhost
  gather_facts: false
  tasks:
  - name: Set a boolean
    set_fact:
      do_fail: true

  - name: "fail"
    fail:
      msg: "Cause a failure"
    when: do_fail
```

10.3.1.2. 环境变量

MigPlan CR 名称和迁移命名空间作为环境变量传递给 hook 容器。这些变量可使用 **lookup** 插件访问。

环境变量示例

```
- hosts: localhost
  gather_facts: false
  tasks:
  - set_fact:
      namespaces: "{{ (lookup( 'env', 'MIGRATION_NAMESPACES')).split(',') }}"

  - debug:
      msg: "{{ item }}"
    with_items: "{{ namespaces }}"

  - debug:
      msg: "{{ lookup( 'env', 'MIGRATION_PLAN_NAME') }}"
```

10.4. 迁移计划选项

您可以在 **MigPlan** 自定义资源 (CR) 中排除、编辑和映射组件。

10.4.1. 排除资源

您可以从 MTC 迁移计划中排除资源，如镜像流、持久性卷（PV）或订阅，以便减少迁移的资源负载，或使用其他工具迁移镜像或 PV。

默认情况下，MTC 会排除服务目录资源和 Operator Lifecycle Manager（OLM）资源。这些资源是服务目录 API 组和 OLM API 组的一部分，目前还不支持迁移。

流程

1. 编辑 **MigrationController** 自定义资源清单：

```
$ oc edit migrationcontroller <migration_controller> -n openshift-migration
```

2. 通过添加参数以排除特定资源，更新 **spec** 部分。对于没有自己的排除参数的资源，请添加 **additional_excluded_resources** 参数：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  disable_image_migration: true 1
  disable_pv_migration: true 2
  additional_excluded_resources: 3
  - resource1
  - resource2
  ...
```

1. 添加 **disable_image_migration: true** 以排除迁移中的镜像流。当 **MigrationController** pod 重启时，**镜像流** 会添加到 **main.yml** 中的 **exclude_resources** 列表中。
2. 添加 **disable_pv_migration: true** 以将 PV 排除在迁移计划之外。当 **MigrationController** pod 重启时，**persistentvolumes** 和 **persistentvolumeclaims** 会添加到 **main.yml** 中的 **exclude_resources** 列表中。禁用 PV 迁移会同时在创建迁移计划时禁用 PV 发现功能。
3. 您可以添加要在 **additional_excluded_resources** 列表中排除的 OpenShift Container Platform 资源。

3. 等待两分钟，使 **MigrationController** Pod 重启，以便应用更改。
4. 验证资源是否排除：

```
$ oc get deployment -n openshift-migration migration-controller -o yaml | grep
EXCLUDED_RESOURCES -A1
```

输出包含排除的资源：

输**出示例**

```
name: EXCLUDED_RESOURCES
value:
resource1,resource2,imagetags,templateinstances,clusterserviceversions,packagemanifests,sul
scriptions,servicebrokers,servicebindings,serviceclasses,serviceinstances,serviceplans,imagest
ams,persistentvolumes,persistentvolumeclaims
```

10.4.2. 映射命名空间

如果您在 **MigPlan** 自定义资源 (CR) 中映射命名空间，您必须确保在源或目标集群上不会重复命名空间，因为命名空间的 UID 和 GID 范围在迁移过程中被复制。

两**个源命名空**间**映射到同一目**标**命名空**间

```
spec:
  namespaces:
    - namespace_2
    - namespace_1:namespace_2
```

如果您希望源命名空间映射到同一名称的命名空间，则不需要创建映射。默认情况下，源命名空间和目标命名空间具有相同的名称。

命名空间**映射不正确**

```
spec:
  namespaces:
    - namespace_1:namespace_1
```

正确的命名空间**引用**

```
spec:
  namespaces:
    - namespace_1
```

10.4.3. 持久性卷声明除外

您可以通过排除您不想迁移的 PVC 来为状态迁移选择持久性卷声明 (PVC)。您可以通过在持久性卷(PV)被发现后设置 **MigPlan** 自定义资源(CR)的 **spec.persistentVolumes.pvc.selection.action** 参数来排除 PVC。

先决条件

- **MigPlan** CR 处于 **Ready** 状态。

流程

- 将 **spec.persistentVolumes.pvc.selection.action** 参数添加到 **MigPlan** CR 中，并将其设置为 **skip** ：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  name: <migplan>
  namespace: openshift-migration
spec:
...
  persistentVolumes:
  - capacity: 10Gi
    name: <pv_name>
    pvc:
...
    selection:
      action: skip
```

10.4.4. 映射持久性卷声明

您可以通过映射 PVC，将持久性卷(PV)数据从源集群迁移到 **MigPlan** CR 中目标集群中已置备的持久性卷声明(PVC)。此映射可确保迁移的应用的目标 PVC 与源 PVC 同步。

您可以在 PV 被发现后，通过更新 **MigPlan** 自定义资源(CR)中的 **spec.persistentVolumes.pvc.name** 参数来映射 PVC。

先决条件

- **MigPlan** CR 处于 **Ready** 状态。

流程

- 更新 **MigPlan** CR 中的 **spec.persistentVolumes.pvc.name** 参数：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  name: <migplan>
  namespace: openshift-migration
spec:
...
```

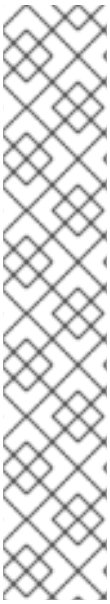
```
persistentVolumes:
- capacity: 10Gi
  name: <pv_name>
  pvc:
    name: <source_pvc>:<destination_pvc> 1
```

1 指定源集群上的 PVC 和目标集群上的 PVC。如果目标 PVC 不存在，则会创建它。您可以在迁移过程中使用此映射更改 PVC 名称。

10.4.5. 编辑持久性卷属性

创建 **MigPlan** 自定义资源(CR)后，**MigrationController** CR 会发现持久性卷(PV)。**spec.persistentVolumes** 块和 **status.destStorageClasses** 块添加到 **MigPlan** CR 中。

您可以编辑 **spec.persistentVolumes.selection** 块中的值。如果您更改了 **spec.persistentVolumes.selection** 块以外的值，当 **MigrationController** CR 协调 **MigPlan** CR 时这些值会被覆盖。



注意

spec.persistentVolumes.selection.storageClass 参数的默认值由以下逻辑决定：

1. 如果源集群 PV 是 Gluster 或 NFS，则默认为 **cephfs**，用于 **accessMode: ReadWriteMany** 或 **cephrbd**，表示 **accessMode: ReadWriteOnce**。
2. 如果 PV 既不是 Gluster，也不是 NFS，*或* **cephfs** 或 **cephrbd** 不可用，则默认为同一调配器的存储类。
3. 如果没有同一置备程序存储类，则默认是目标集群的默认存储类。

您可以将 **storageClass** 值改为 **MigPlan** CR 的 **status.destStorageClasses** 块中任何 **name** 参数的值。

如果 **storageClass** 值为空，则 PV 在迁移后将没有存储类。例如，当您想要将 PV 移到目标集群上的 NFS 卷时，这个选项是合适的。

先决条件

- **MigPlan** CR 处于 **Ready** 状态。

流程

- 编辑 **MigPlan** CR 中的 **spec.persistentVolumes.selection** 值：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  name: <migplan>
  namespace: openshift-migration
spec:
  persistentVolumes:
  - capacity: 10Gi
    name: pvc-095a6559-b27f-11eb-b27f-021bddcaf6e4
    proposedCapacity: 10Gi
```

```
    pvc:
      accessModes:
      - ReadWriteMany
      hasReference: true
      name: mysql
      namespace: mysql-persistent
    selection:
      action: <copy> (1)
      copyMethod: <filesystem> (2)
      verify: true (3)
      storageClass: <gp2> (4)
      accessMode: <ReadWriteMany> (5)
    storageClass: cephfs
```

1. 允许的值包括 **move**、**copy** 和 **skip**。如果只支持一个操作，则默认值是支持的动作。如果支持多个操作，则默认值为 **copy**。
2. 允许的值是 **snapshot** 和 **filesystem**。默认值为 **filesystem**。
3. 如果您在 MTC web 控制台中为文件系统复制选择了验证选项，则会显示 **verify** 参数。您可以将其设置为 **false**。
4. 您可以将默认值改为 **MigPlan** CR 的 **status.destStorageClasses** 块中任何 **name** 参数的值。如果没有指定值，则 PV 在迁移后没有存储类。
5. 允许的值有 **ReadWriteOnce** 和 **ReadWriteMany**。如果没有指定这个值，则默认值是源集群 PVC 的访问模式。您只能在 **MigPlan** CR 中编辑访问模式。您不能使用 MTC web 控制台进行编辑。

10.4.6. 转换 MTC web 控制台中的存储类

您可以在同一个集群中迁移持久性卷(PV)的存储类来转换它。要做到这一点，您必须在 Migration Toolkit for Containers(MTC)web 控制台中创建并运行迁移计划。

先决条件

- 您必须在 MTC 的集群中以具有 **cluster-admin** 权限的用户身份登录。
- 您必须在 MTC web 控制台中添加集群。

流程

1. 在 OpenShift Container Platform Web 控制台的左侧导航窗格中，点 **Projects**。
2. 在项目列表中点击您的项目。
   此时会打开 **Project 详情**页面。
3. 点 **DeploymentConfig** 名称。记录其正在运行的 Pod 的名称。
4. 打开项目的 YAML 选项卡。查找 PV 并记下其对应的持久性卷声明(PVC)的名称。
5. 在 MTC web 控制台中点 **Migration Plan**。
6. 点 **Add migration plan**。

7. 输入 **Plan 名称**。
迁移计划名称必须包含 3 到 63 个小写字母数字字符(**a-z，0-9**)且不得包含空格或下划线(_)。

8. 在 **Migration type** 菜单中，选择 **Storage class conversion**。

9. 从 **Source 集群**列表中，选择所需的集群进行存储类转换。

10. 点击 **Next**。
Namespaces 页面将打开。

11. 选择所需的项目。

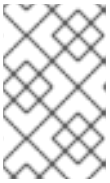
12. 点击 **Next**。
此时会打开 **Persistent volumes** 页面。页面中显示项目中 PV，默认选中的所有 PV。

13. 对于每个 PV，选择所需的目标存储类。

14. 点击 **Next**。
该向导会验证新的迁移计划，并显示它已就绪。

15. 单击 **Close**。
新计划会出现在 **Migration Plan** 页面中。

16. 要开始转换，请点击新计划的选项菜单。
在 **Migrations** 下会显示两个选项，即 **Stage** 和 **Cutover**。



注意

在应用程序中剪切迁移更新 PVC 引用。

阶段迁移不会更新应用程序中的 PVC 引用。

17. 选择所需选项。
根据您选择的选项，显示 **Stage migration** 或 **Cutover migration** 通知。

18. 点 **Migrate**。
根据您选择的选项，**Stage started** 或 **Cutover started** 消息会显示。

19. 要查看当前迁移的状态，请点击 **Migrations** 列中的数量。
此时会打开 **Migrations** 页面。

20. 要查看有关当前迁移和监控其进度的更多详细信息，请从 **Type** 列选择迁移。
此时会打开 **Migration 详情**页面。当迁移进入 DirectVolume 步骤时，步骤的状态将变为 **Running Rsync Pods to migrate Persistent Volume data**，您可以点 **View details** 并查看副本的详细状态。

21. 在面包屑导航栏中，点 **Stage** 或 **Cutover**，并等待所有步骤完成。

22. 打开 OpenShift Container Platform Web 控制台的 **PersistentVolumeClaims** 选项卡。
您可以看到新 PVC 名称，但以 **new** 结尾（使用目标存储类）。

23. 在左侧导航窗格中，点 **Pods**。查看您的项目的 pod 已再次运行。

其他资源

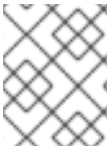
- 有关 **move** 和 **copy** 操作的详情，请参考 MTC 工作流。

- 有关 **skip** 操作的详情，请参阅从迁移中排除 PVC。
- 有关文件系统和快照复制方法的详情，请参阅关于数据复制方法。

10.4.7. 使用 MTC API 执行 Kubernetes 对象的状态迁移

迁移所有 PV 数据后，您可以使用 Migration Toolkit for Containers (MTC) API 执行组成应用程序的 Kubernetes 对象的一次性状态迁移。

您可以通过配置 **MigPlan** 自定义资源 (CR) 字段来提供一个带有额外标签选择器的 Kubernetes 资源列表来进一步过滤这些资源，然后通过创建 **MigMigration** CR 来执行迁移。**MigPlan** 资源在迁移后关闭。



注意

选择 Kubernetes 资源是一个仅限 API 的功能。您必须更新 **MigPlan** CR，并使用 CLI 为它创建一个 **MigMigration** CR。MTC web 控制台不支持迁移 Kubernetes 对象。

注意

迁移后，**MigPlan** CR 的 **closed** 参数被设置为 **true**。您不能为此 **MigPlan** CR 创建另一个 **MigMigration** CR。

使用以下选项之一将 Kubernetes 对象添加到 **MigPlan** CR 中：

- 将 Kubernetes 对象添加到 **includeResources** 部分。当 **MigPlan** CR 中指定 **includedResources** 字段时，计划会将 **group-kind** 的列表作为输入。只有列表中显示的资源才会包含在迁移中。
- 添加可选的 **labelSelector** 参数，以过滤 **MigPlan** 中的 **includedResources**。当指定此字段时，迁移中仅包含与标签选择器匹配的资源。例如，您可以使用标签 **app: frontend** 作为过滤器来过滤 **Secret** 和 **ConfigMap** 资源列表。

流程

1. 更新 **MigPlan** CR，使其包含 Kubernetes 资源，并可选择性地通过添加 **labelSelector** 参数来过滤包含的资源：
   a. 更新 **MigPlan** CR 使其包含 Kubernetes 资源：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  name: <migplan>
  namespace: openshift-migration
spec:
  includedResources:
  - kind: <kind> 1
    group: ""
  - kind: <kind>
    group: ""
```

1 指定 Kubernetes 对象，如 **Secret** 或 **ConfigMap**。

   b. 可选：要通过添加 **labelSelector** 参数来过滤包含的资源：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  name: <migplan>
  namespace: openshift-migration
spec:
  includedResources:
  - kind: <kind> 1
    group: ""
  - kind: <kind>
    group: ""
...
  labelSelector:
    matchLabels:
      <label> 2
```

1. 指定 Kubernetes 对象，如 **Secret** 或 **ConfigMap**。
2. 指定要迁移的资源标签，如 **app: frontend**。

2. 创建一个 **MigMigration** CR 来迁移所选 Kubernetes 资源。验证 **migPlanRef** 引用了了正确的 **MigPlan** ：

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  generateName: <migplan>
  namespace: openshift-migration
spec:
  migPlanRef:
    name: <migplan>
    namespace: openshift-migration
  stage: false
```

10.5. 迁移控制器选项

您可以编辑迁移计划限制，启用持久性卷大小，或者在 **MigrationController** 自定义资源 (CR) 中启用缓存的 Kubernetes 客户端，以用于大型迁移并提高性能。

10.5.1. 为大型迁移增加限制

您可以使用 MTC 为大型迁移增加迁移对象和容器资源的限制。

重要

您必须在生产环境中执行迁移前测试这些更改。

流程

1. 编辑 **MigrationController** 自定义资源（CR）清单：

```
$ oc edit migrationcontroller -n openshift-migration
```

2. 更新以下参数：

```
...
mig_controller_limits_cpu: "1" 1
mig_controller_limits_memory: "10Gi" 2
...
mig_controller_requests_cpu: "100m" 3
mig_controller_requests_memory: "350Mi" 4
...
mig_pv_limit: 100 5
mig_pod_limit: 100 6
mig_namespace_limit: 10 7
...
```

1. 指定 **MigrationController** CR 可用的 CPU 数量。
2. 指定 **MigrationController** CR 可用的内存量。
3. 指定可用于 **MigrationController** CR 请求的 CPU 单元数。**100m** 代表 0.1 CPU 单元（100 * 1e-3）。
4. 指定可用于 **MigrationController** CR 请求的内存量。
5. 指定可迁移的持久性卷数量。
6. 指定可迁移的 pod 数量。
7. 指定可迁移的命名空间数量。

3. 创建使用更新的参数验证更改的迁移计划。
如果您的迁移计划超过 **MigrationController** CR 限制，则 MTC 控制台在保存迁移计划时会显示警告信息。

10.5.2. 为直接卷迁移启用持久性卷大小

您可以启用持久性卷（PV）调整直接卷迁移的大小，以避免在目标集群中耗尽磁盘空间。

当 PV 的磁盘用量达到配置级别时，**MigrationController** 自定义资源（CR）会将持久性卷声明（PVC）的请求存储容量与其实际置备的容量进行比较。然后，它会计算目标集群所需的空间。

pv_resizing_threshold 参数决定何时使用 PV 调整大小。默认阈值是 **3%**。这意味着，当 PV 的磁盘用量超过 **97%** 时，PV 会调整大小。您可以提高这个阈值，以便 PV 调整大小在较低的磁盘用量级别上发生。

PVC 容量根据以下标准计算：

- 如果 PVC 请求的存储容量（**spec.resources.requests.storage**）不等于实际置备的容量（**status.capacity.storage**），则会使用较大的值。
- 如果 PV 通过 PVC 置备，然后更改以便其 PV 和 PVC 容量不再匹配，则会使用较大的值。

先决条件

- PVC 必须附加到一个或多个正在运行的 pod，以便 **MigrationController** CR 可以执行命令。

流程

1. 登录主机集群。
2. 通过修补 **MigrationController** CR 来启用 PV 调整大小：

```
$ oc patch migrationcontroller migration-controller -p '{"spec":
{"enable_dvm_pv_resizing":true}}' \ 1
  --type='merge' -n openshift-migration
```

1 将值设为 **false** 可禁用 PV 大小调整。

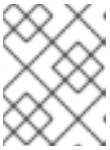
3. 可选：更新 **pv_resizing_threshold** 参数以增加阈值：

```
$ oc patch migrationcontroller migration-controller -p '{"spec":{"pv_resizing_threshold":41}}' \
1
  --type='merge' -n openshift-migration
```

1 默认值为 **3**。

超过阈值时，**MigPlan** CR 状态中会显示以下状态信息：

```
status:
  conditions:
...
  - category: Warn
    durable: true
    lastTransitionTime: "2021-06-17T08:57:01Z"
    message: 'Capacity of the following volumes will be automatically adjusted to avoid disk
capacity issues in the target cluster:  [pvc-b800eb7b-cf3b-11eb-a3f7-0eae3e0555f3]'
    reason: Done
    status: "False"
    type: PvCapacityAdjustmentRequired
```



注意

对于 AWS gp2 存储，因为 gp2 计算卷用量和大小的方式，这个信息不会出现，除非 **pv_resizing_threshold** 为 42% 或更高。（BZ#1973148）

10.5.3. 启用缓存的 Kubernetes 客户端

您可以在 **MigrationController** 自定义资源（CR）中启用缓存的 Kubernetes 客户端，以便在迁移过程中提高性能。在位于不同区域的集群之间迁移时，或存在显著的网络延迟时，会显示最大的性能优势。

注意

但是，委派的任务（例如，用于直接卷迁移的 Rsync 备份或 Velero 备份和恢复）并不会显著提高通过缓存的客户端的性能。

缓存的客户端需要额外的内存，因为 **MigrationController** CR 会缓存与 **MigCluster** CR 交互所需的所有 API 资源。通常发送到 API 服务器的请求会被定向到缓存。缓存会监视 API 服务器是否有更新。

如果启用了缓存的客户端后发生 **OOMKilled** 错误，您可以增加 **MigrationController** CR 的内存限值和请求。

流程

1. 运行以下命令启用缓存的客户端：

```
$ oc -n openshift-migration patch migrationcontroller migration-controller --type=json --patch \
  '[{ "op": "replace", "path": "/spec/mig_controller_enable_cache", "value": true}]'
```

2. 可选：运行以下命令来增加 **MigrationController** CR 内存限值：

```
$ oc -n openshift-migration patch migrationcontroller migration-controller --type=json --patch \
  '[{ "op": "replace", "path": "/spec/mig_controller_limits_memory", "value": <10Gi>}]'
```

3. 可选：运行以下命令来增加 **MigrationController** CR 内存请求：

```
$ oc -n openshift-migration patch migrationcontroller migration-controller --type=json --patch \
  '[{ "op": "replace", "path": "/spec/mig_controller_requests_memory", "value": <350Mi>}]'
```

第 11 章 故障排除

本节论述了对 Migration Toolkit for Containers（MTC）进行故障排除的资源。

有关已知问题，请参阅 MTC 发行注记。

11.1. MTC 工作流

您可以使用 MTC web 控制台或 Kubernetes API 将 Kubernetes 资源、持久性卷数据和内部容器镜像迁移到 OpenShift Container Platform 4.15。

MTC 迁移以下资源：

- 在迁移计划中指定的命名空间。
- 命名空间范围的资源：当 MTC 迁移命名空间时，它会迁移与该命名空间关联的所有对象和资源，如服务或 Pod。另外，如果一个资源在命名空间中存在但不在集群级别，这个资源依赖于集群级别存在的另外一个资源，MTC 会迁移这两个资源。
  例如，安全性上下文约束（SCC）是一个存在于集群级别的资源，服务帐户（SA）是存在于命名空间级别的资源。如果 MTC 迁移的命名空间中存在 SA，MTC 会自动找到链接到 SA 的所有 SCC，并迁移这些 SCC。同样，MTC 会迁移链接到命名空间持久性卷声明的持久性卷。

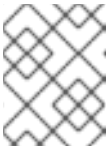
  注意

  根据资源，可能需要手动迁移集群范围的资源。

- 自定义资源 (CR) 和自定义资源定义 (CRD)：MTC 在命名空间级别自动迁移 CR 和 CRD。

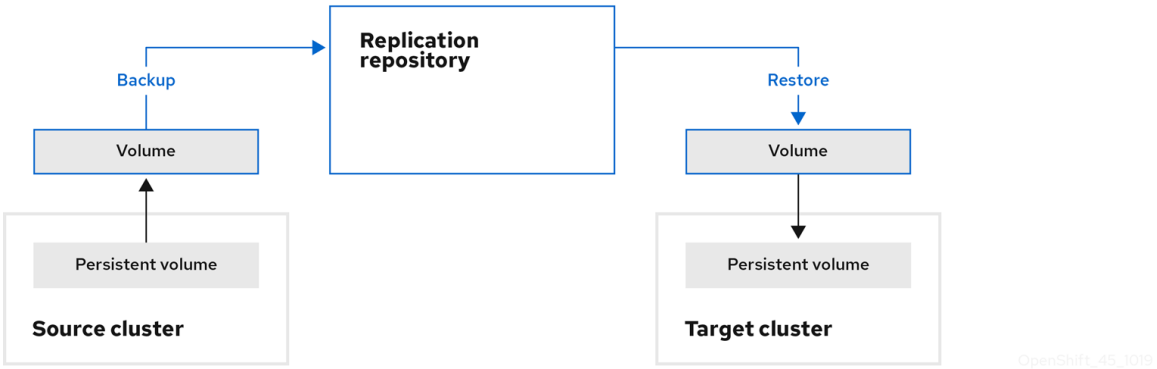
使用 MTC Web 控制台迁移应用程序涉及以下步骤：

1. 在所有集群中安装 MTC Operator。
   您可以在有限的或没有互联网访问的受限环境中为 Containers Operator 安装 Migration Toolkit。源和目标集群必须可以在相互间进行访问，而需要可以访问 registry 的镜像（mirror）.
2. 配置复制存储库，这是 MTC 用来迁移数据的中间对象存储。
   源和目标集群必须有对复制仓库的不受限制的网络访问权限。如果使用代理服务器，您必须将其配置为允许复制仓库和集群间的网络流量。
3. 在 MTC web 控制台中添加源集群。
4. 在 MTC web 控制台中添加复制存储库。
5. 创建迁移计划，包含以下数据迁移选项之一：
   - **Copy**：MTC 将数据从源集群复制到复制存储库，再从复制存储库把数据复制到目标集群。

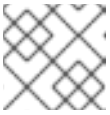
     

     注意

     如果您使用直接镜像迁移或直接卷迁移，则镜像或卷会直接从源集群复制到目标集群。



- **Move**：MTC 从源集群中卸载一个远程卷（例如 NFS），在目标集群上创建一个指向这个远程卷的 PV 资源，然后在目标集群中挂载远程卷。在目标集群中运行的应用程序使用源集群使用的同一远程卷。远程卷必须可以被源集群和目标集群访问。



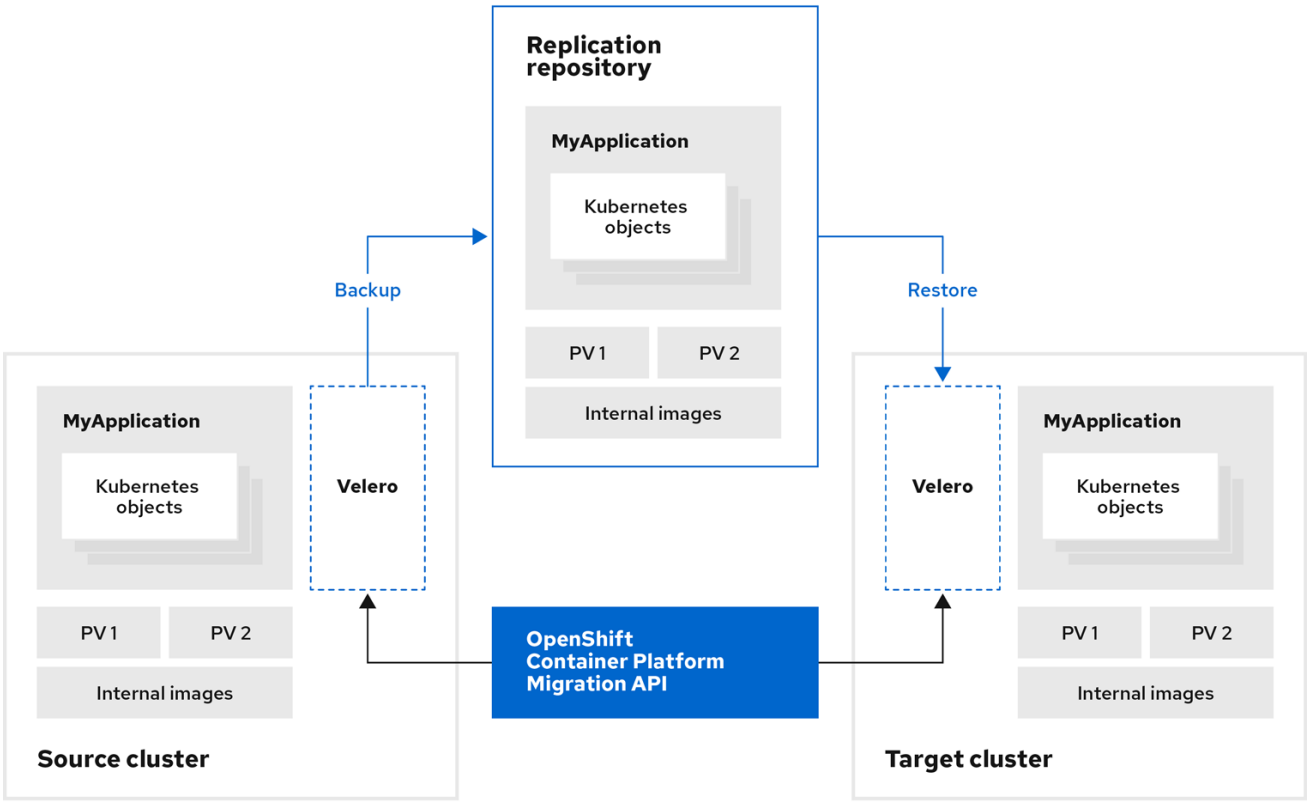
注意

虽然复制仓库没有出现在此图表中，但迁移需要它。

6. 运行迁移计划，使用以下选项之一：

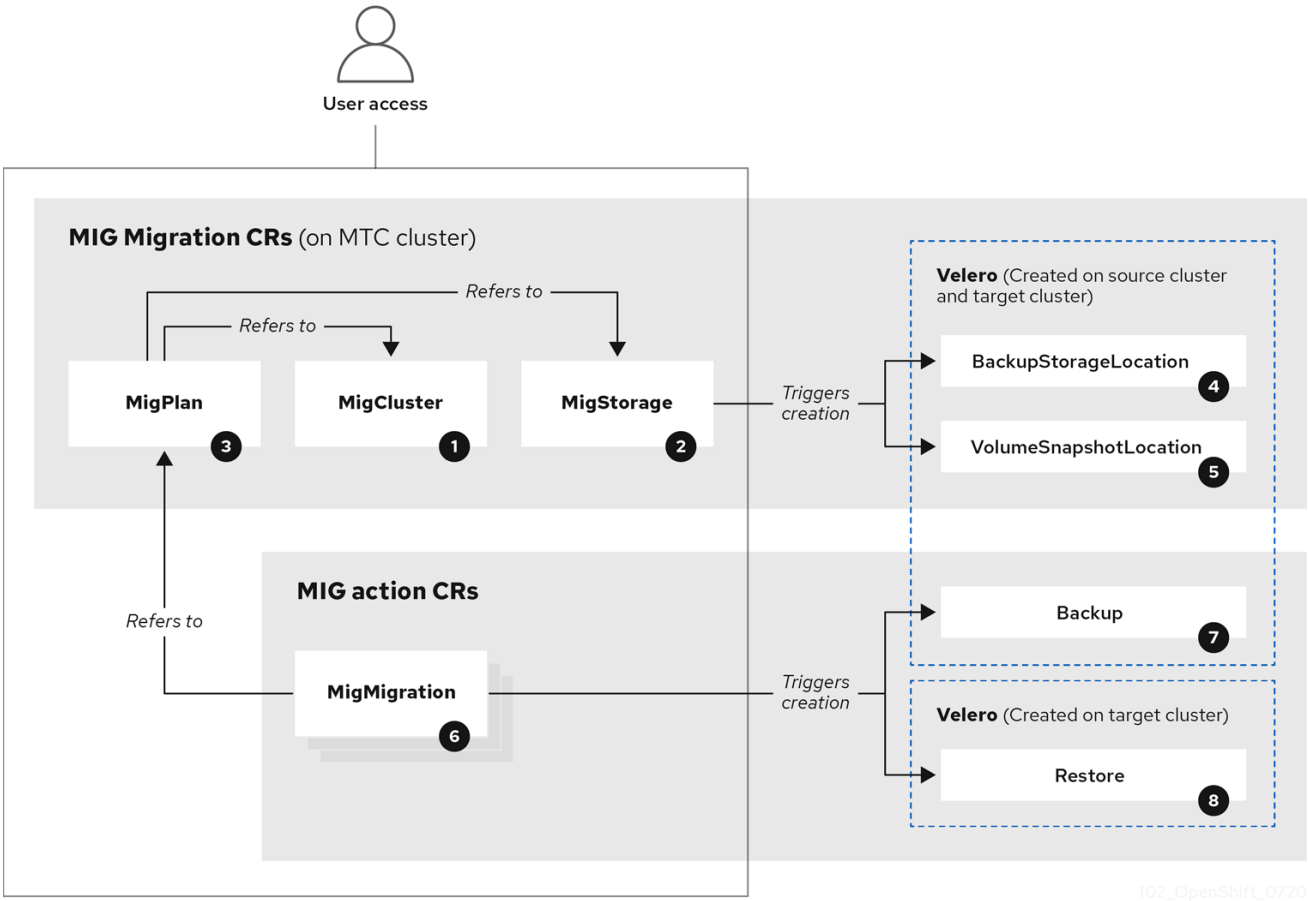
- **stage** 在不停止应用程序的情况下将数据复制到目标集群。
  阶段迁移可以多次运行，以便在迁移前将大多数数据复制到目标。运行一个或多个阶段迁移可缩短迁移的持续时间。

- **cutover** 会停止源集群上的应用程序，并将资源移到目标集群。
  可选：您可以清除 **Halt transactions on the source cluster during migration**多选设置。



关于 MTC 自定义资源

MTC 会创建以下自定义资源（CR）：



1 MigCluster （配置, MTC 集群）: 集群定义

2 MigStorage （配置, MTC 集群）: 存储定义

3 MigPlan （配置, MTC 集群）: 迁移计划

MigPlan CR 描述了要迁移的源和目标集群、复制仓库和命名空间。它与 0 个、1 个或多个 **MigMigration** CR 关联。

注意

删除 **MigPlan** CR 会删除关联的 **MigMigration** CR。

4 BackupStorageLocation （配置, MTC 集群）: **Velero** 备份对象的位置

5 VolumeSnapshotLocation （配置, MTC 集群）: **Velero** 卷快照的位置

6 MigMigration （操作，MTC 集群）：Migration，在每次进行 stage 或迁移数据时创建。每个 **MigMigration** CR 都与 **MigPlan** CR 关联。

7 Backup（操作，源集群）：当运行迁移计划时，**MigMigration** CR 在每个源集群上创建两个 **Velero** 备份 CR：

- 备份 CR #1 用于Kubernetes 对象
- 备份 CR #2 用于 PV 数据

8 Restore （操作，目标集群）：在运行迁移计划时，**MigMigration** CR 在目标集群上创建两个 **Velero** 恢复 CR：

- 恢复 CR #1（使用备份 CR #2）用于 PV 数据
- 恢复 CR #2（使用备份 CR #1）用于 Kubernetes 对象

11.2. MTC 自定义资源清单

MTC 使用以下自定义资源（CR）清单来迁移应用程序。

11.2.1. DirectImageMigration

DirectImageMigration CR 直接将镜像从源集群复制到目标集群。

```
apiVersion: migration.openshift.io/v1alpha1
kind: DirectImageMigration
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <direct_image_migration>
spec:
  srcMigClusterRef:
```

```
    name: <source_cluster>
    namespace: openshift-migration
  destMigClusterRef:
    name: <destination_cluster>
    namespace: openshift-migration
  namespaces: (1)
    - <source_namespace_1>
    - <source_namespace_2>:<destination_namespace_3> (2)
```

1. 包含要迁移的镜像的一个或多个命名空间。默认情况下，目标命名空间的名称与源命名空间相同。
2. 使用不同名称映射到目标命名空间的源命名空间。

11.2.2. DirectImageStreamMigration

DirectImageStreamMigration CR 直接将镜像流引用从源集群复制到目标集群。

```
apiVersion: migration.openshift.io/v1alpha1
kind: DirectImageStreamMigration
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <direct_image_stream_migration>
spec:
  srcMigClusterRef:
    name: <source_cluster>
    namespace: openshift-migration
  destMigClusterRef:
    name: <destination_cluster>
    namespace: openshift-migration
  imageStreamRef:
    name: <image_stream>
    namespace: <source_image_stream_namespace>
  destNamespace: <destination_image_stream_namespace>
```

11.2.3. DirectVolumeMigration

DirectVolumeMigration CR 直接将持久性卷（PV）从源集群复制到目标集群。

```
apiVersion: migration.openshift.io/v1alpha1
kind: DirectVolumeMigration
metadata:
  name: <direct_volume_migration>
  namespace: openshift-migration
spec:
  createDestinationNamespaces: false (1)
  deleteProgressReportingCRs: false (2)
  destMigClusterRef:
    name: <host_cluster> (3)
    namespace: openshift-migration
  persistentVolumeClaims:
  - name: <pvc> (4)
    namespace: <pvc_namespace>
```

```
  srcMigClusterRef:
    name: <source_cluster>
    namespace: openshift-migration
```

1. 设置为 **true**，为目标集群上的 PV 创建命名空间。
2. 设置为 **true**，以在迁移后删除 **DirectVolumeMigrationProgress** CR。默认值为 **false**，保留 **DirectVolumeMigrationProgress** CR 以进行故障排除。
3. 如果目标集群不是主机集群，请更新集群名称。
4. 指定要迁移的一个或多个 PVC。

11.2.4. DirectVolumeMigrationProgress

DirectVolumeMigrationProgress CR 显示 **DirectVolumeMigration** CR 的进度。

```
apiVersion: migration.openshift.io/v1alpha1
kind: DirectVolumeMigrationProgress
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <direct_volume_migration_progress>
spec:
  clusterRef:
    name: <source_cluster>
    namespace: openshift-migration
  podRef:
    name: <rsync_pod>
    namespace: openshift-migration
```

11.2.5. MigAnalytic

MigAnalytic CR 从关联的 **MigPlan** CR 收集镜像、Kubernetes 资源和持久性卷（PV）容量的数量。

您可以配置它收集的数据。

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigAnalytic
metadata:
  annotations:
    migplan: <migplan>
  name: <miganalytic>
  namespace: openshift-migration
  labels:
    migplan: <migplan>
spec:
  analyzeImageCount: true (1)
  analyzeK8SResources: true (2)
  analyzePVCapacity: true (3)
  listImages: false (4)
  listImagesLimit: 50 (5)
```

```
  migPlanRef:
    name: <migplan>
    namespace: openshift-migration
```

1. 可选：返回镜像数量。
2. 可选：返回 Kubernetes 资源的数量、类型和 API 版本。
3. 可选：返回 PV 容量。
4. 返回镜像名称列表。默认为 **false**，因此输出不会过长。
5. 可选：指定如果 **listImages** 为 **true** 时要返回的最大镜像名称数。

11.2.6. MigCluster

MigCluster CR 定义一个主机、本地或远程集群。

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigCluster
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <host_cluster> 1
  namespace: openshift-migration
spec:
  isHostCluster: true 2
# The 'azureResourceGroup' parameter is relevant only for Microsoft Azure.
  azureResourceGroup: <azure_resource_group> 3
  caBundle: <ca_bundle_base64> 4
  insecure: false 5
  refresh: false 6
# The 'restartRestic' parameter is relevant for a source cluster.
  restartRestic: true 7
# The following parameters are relevant for a remote cluster.
  exposedRegistryPath: <registry_route> 8
  url: <destination_cluster_url> 9
  serviceAccountSecretRef:
    name: <source_secret> 10
    namespace: openshift-config
```

1. 如果 **migration-controller** pod 没有在这个集群中运行，请更新集群名称。
2. 如果为 **true**，则 **migration-controller** pod 在此集群中运行。
3. 仅 Microsoft Azure：指定资源组。
4. 可选：如果您为自签名 CA 证书创建了一个证书捆绑包，且 **insecure** 参数值为 **false**，请指定 base64 编码的证书捆绑包。
5. 设置为 **true** 以禁用 SSL 验证。
6. 设置为 **true** 以验证集群。

7 设置为 **true**，以在创建 **Stage** pod 后重启源集群中的 **Restic** pod。

8 远程集群和直接镜像迁移：指定公开的安全 registry 路径。

9 仅远程集群：指定 URL。

10 仅远程集群：指定 **Secret** 对象的名称。

11.2.7. MigHook

MigHook CR 定义一个迁移 hook，它在迁移的指定阶段运行自定义代码。您可以创建最多四个迁移 hook。每个 hook 在迁移的不同阶段运行。

您可以配置 hook 名称、运行时持续时间、自定义镜像，以及 hook 将运行的集群。

hook 的迁移阶段和命名空间在 **MigPlan** CR 中配置。

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigHook
metadata:
  generateName: <hook_name_prefix> 1
  name: <mighook> 2
  namespace: openshift-migration
spec:
  activeDeadlineSeconds: 1800 3
  custom: false 4
  image: <hook_image> 5
  playbook: <ansible_playbook_base64> 6
  targetCluster: source 7
```

1 可选：此参数的值后附加一个唯一的哈希值，以便每个迁移 hook 都有一个唯一的名称。您不需要指定 **name** 参数的值。

2 指定迁移 hook 名称，除非指定了 **generateName** 参数的值。

3 可选：指定 hook 可运行的最大秒数。默认值为 **1800**。

4 如果为 **true**，则 hook 是一个自定义镜像。自定义镜像可以包括 Ansible，也可以使用不同的编程语言编写。

5 指定自定义镜像，例如 **quay.io/konveyor/hook-runner:latest**。如果 **custom** 是 **true**，则需要此项。

6 base64 编码的 Ansible playbook.如果 **custom** 是 **false**，则必需。

7 指定要运行 hook 的集群。有效值为 **source** 或 **destination**。

11.2.8. MigMigration

MigMigration CR 运行一个 **MigPlan** CR。

您可以配置 **Migmigration** CR，以运行一个阶段或增量迁移，取消正在进行中的迁移，或回滚已完成的迁移。

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <migmigration>
  namespace: openshift-migration
spec:
  canceled: false (1)
  rollback: false (2)
  stage: false (3)
  quiescePods: true (4)
  keepAnnotations: true (5)
  verify: false (6)
  migPlanRef:
    name: <migplan>
    namespace: openshift-migration
```

1. 设置为 **true** 可取消正在进行中的迁移。
2. 设置为 **true** 以回滚已完成的迁移。
3. 设置为 **true** 以运行暂存迁移。数据会被递增复制，pod 不会在源集群中停止。
4. 设置为 **true** 可在迁移期间停止应用程序。在备份阶段后，源集群中的 pod 被缩减为 **0**。
5. 设置为 **true** 以保留迁移过程中应用的标签和注解。
6. 设置为 **true**，以检查目标集群中迁移的 pod 的状态，并返回处于 **Running** 状态的 pod 名称。

11.2.9. MigPlan

MigPlan CR 定义迁移计划的参数。

您可以配置目标命名空间、hook 阶段以及直接或间接迁移。

注意

默认情况下，目标命名空间的名称与源命名空间相同。如果配置了一个不同的目标命名空间，您必须确保不会在源或目标集群上重复命名空间，因为在迁移过程中复制了 UID 和 GID 范围。

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigPlan
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <migplan>
  namespace: openshift-migration
spec:
  closed: false (1)
  srcMigClusterRef:
    name: <source_cluster>
```

```
  namespace: openshift-migration
destMigClusterRef:
  name: <destination_cluster>
  namespace: openshift-migration
hooks: 2
  - executionNamespace: <namespace> 3
    phase: <migration_phase> 4
    reference:
      name: <hook> 5
      namespace: <hook_namespace> 6
    serviceAccount: <service_account> 7
indirectImageMigration: true 8
indirectVolumeMigration: false 9
migStorageRef:
  name: <migstorage>
  namespace: openshift-migration
namespaces:
  - <source_namespace_1> 10
  - <source_namespace_2>
  - <source_namespace_3>:<destination_namespace_4> 11
refresh: false 12
```

1. 如果为 **true**，则迁移已完成。您不能为此 **MigPlan** CR 创建另一个 **MigMigration** CR。
2. 可选：最多可指定四个迁移 hook。每个 hook 必须在不同的迁移阶段运行。
3. 可选：指定运行 hook 的命名空间。
4. 可选：指定 hook 运行期间的迁移阶段。一个 hook 可以分配给一个阶段。有效值为 **PreBackup**、**PostBackup**、**PreRestore** 和 **PostRestore**。
5. 可选：指定 **MigHook** CR 的名称。
6. 可选：指定 **MigHook** CR 的命名空间。
7. 可选：指定一个具有 **cluster-admin** 权限的服务帐户。
8. 如果为 **true**，则禁用直接镜像迁移。镜像从源集群复制到复制存储库，并从复制存储库复制到目标集群。
9. 如果为 **true**，则禁用直接卷迁移。PV 从源集群复制到复制存储库，再从复制存储库复制到目标集群。
10. 指定一个或多个源命名空间。如果只指定源命名空间，则目标命名空间是相同的。
11. 如果目标命名空间与源命名空间不同，请指定它。
12. 如果为 **true** ， **MigPlan** CR 会被验证。

11.2.10. MigStorage

MigStorage CR 描述了复制存储库的对象存储。

支持 Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Storage、Multi-Cloud Object Gateway 和通用 S3 兼容云存储。

AWS 和快照复制方法具有额外的参数。

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigStorage
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <migstorage>
  namespace: openshift-migration
spec:
  backupStorageProvider: <backup_storage_provider> 1
  volumeSnapshotProvider: <snapshot_storage_provider> 2
  backupStorageConfig:
    awsBucketName: <bucket> 3
    awsRegion: <region> 4
    credsSecretRef:
      namespace: openshift-config
      name: <storage_secret> 5
    awsKmsKeyId: <key_id> 6
    awsPublicUrl: <public_url> 7
    awsSignatureVersion: <signature_version> 8
  volumeSnapshotConfig:
    awsRegion: <region> 9
    credsSecretRef:
      namespace: openshift-config
      name: <storage_secret> 10
  refresh: false 11
```

1. 指定存储供应商。
2. 仅快照复制方法：指定存储供应商。
3. 仅 AWS：指定存储桶名称。
4. 仅 AWS：指定存储桶区域，如 **us-east-1**。
5. 指定您为存储创建的 **Secret** 对象的名称。
6. 仅 AWS：如果您使用 AWS 密钥管理服务，请指定该密钥的唯一标识符。
7. 仅 AWS：如果授予 AWS 存储桶的公共访问权限，请指定存储桶 URL。
8. 仅 AWS：指定向存储桶验证请求的 AWS 签名版本，例如 **4**。
9. 仅快照复制方法：指定集群的地理位置。
10. 仅快照复制方法：指定您为存储创建的 **Secret** 对象的名称。
11. 设置为 **true** 以验证集群。

11.3. 日志和调试工具

本节论述了可用于故障排除的日志和调试工具。

11.3.1. 查看迁移计划资源

您可以使用 MTC web 控制台和命令行界面（CLI）查看迁移计划资源来监控正在运行的迁移或排除迁移失败的问题。

流程

1. 在 MTC web 控制台中点 **Migration Plans**。
2. 点迁移计划旁边的 **Migrations** 编号来查看 **Migrations** 页面。
3. 点击迁移以查看**迁移详情**。
4. 扩展 **迁移资源**，以在树视图中查看迁移资源及其状态。

注意

要对失败的迁移进行故障排除，请从失败的高级别资源开始，然后向下级资源组成资源树。

5. 点击资源  旁边的 Options 菜单并选择以下选项之一：
   - **复制 oc describe 命令**将命令复制到您的剪贴板。
     - 登录相关集群，然后运行命令。
       资源的条件和事件以 YAML 格式显示。
   - **复制 oc logs 命令**将命令复制到您的剪贴板。
     - 登录相关集群，然后运行命令。
       如果资源支持日志过滤，则会显示过滤的日志。
   - **View JSON** 在 Web 浏览器中以 JSON 格式显示资源数据。
     其数据与 **oc get <resource>** 命令的输出结果相同。

11.3.2. 查看迁移计划日志

您可以查看迁移计划的聚合日志。您可以使用 MTC web 控制台将命令复制到剪贴板中，然后从命令行界面（CLI）运行命令。

该命令显示以下 pod 的过滤日志：

- **Migration Controller**
- **Velero**
- **Restic**
- **Rsync**

- **Stunnel**
- **容器镜像仓库（Registry）**

流程

1. 在 MTC web 控制台中点 **Migration Plans**。
2. 点迁移计划旁边的 **Migrations** 号。
3. 单击 **View logs**。
4. 点击 Copy 图标将 **oc logs** 命令复制到您的剪贴板。
5. 登录到相关的集群并在 CLI 中输入命令。
   此时会显示迁移计划的聚合日志。

11.3.3. 使用迁移日志读取器

您可以使用迁移日志读取器显示所有迁移日志的过滤视图。

流程

1. 获取 **mig-log-reader** pod:

```
$ oc -n openshift-migration get pods | grep log
```

2. 输入以下命令显示单个迁移日志：

```
$ oc -n openshift-migration logs -f <mig-log-reader-pod> -c color
```
(1)

(1) **-c plain** 选项显示没有颜色的日志。

11.3.4. 访问性能指标

MigrationController 自定义资源 (CR) 记录指标数据，并将它们拉取到集群监控存储中。您可以使用 Prometheus Query Language (PromQL) 来诊断迁移性能问题，以此查询指标数据。当 Migration Controller pod 重启时，会重置所有指标。

您可以使用 OpenShift Container Platform Web 控制台访问性能指标并运行查询。

流程

1. 在 OpenShift Container Platform web 控制台中点 **Observe → Metrics**。
2. 输入 PromQL 查询，选择一个要显示的时间窗口，然后单击 **Run Queries**。
   如果您的 Web 浏览器没有显示所有结果，请使用 Prometheus 控制台。

11.3.4.1. 提供的指标

MigrationController 自定义资源 (CR) 提供了 **MigMigration** CR 计数及其 API 请求的指标。

11.3.4.1.1. cam_app_workload_migrations

此指标是一段时间内的 **MigMigration** CR 计数。它可用于与 **mtc_client_request_count** 和 **mtc_client_request_elapsed** 指标一起查看，以整理迁移状态变化的 API 请求信息。此指标包含在 Telemetry 中。

表 11.1. cam_app_workload_migrations metric

可查询的标签名称	标签值示例	标签描述
status	**running**, **idle**, **failed**, **completed**	**MigMigration** CR 的状态
type	stage, final	**MigMigration** CR 类型

11.3.4.1.2. mtc_client_request_count

此指标是 **MigrationController** 发布的 Kubernetes API 请求的累积计数。它不包含在 Telemetry 中。

表 11.2. mtc_client_request_count metric

可查询的标签名称	标签值示例	标签描述
cluster	**https://migcluster-url:443**	针对发出请求的集群
component	**MigPlan**, **MigCluster**	发出请求的子控制器 API
function	**(*ReconcileMigPlan).Reconcile**	发出请求的功能
kind	**SecretList**、**Deployment**	为 Kubernetes 发出的请求类型

11.3.4.1.3. mtc_client_request_elapsed

这个指标是 **MigrationController** 发布的 Kubernetes API 请求的累积延迟，以毫秒为单位。它不包含在 Telemetry 中。

表 11.3. mtc_client_request_elapsed 指标

可查询的标签名称	标签值示例	标签描述
cluster	**https://cluster-url.com:443**	针对发出请求的集群
component	**migplan**, **migcluster**	发出请求的子控制器 API
function	**(*ReconcileMigPlan).Reconcile**	发出请求的功能
kind	**SecretList**、**Deployment**	为请求发布的 Kubernetes 资源

11.3.4.1.4. 有用的查询

表格中列出了可用于监控性能的一些有用查询。

表 11.4. 有用的查询

查询	描述
mtc_client_request_count	发布的 API 请求数，按请求类型排序
sum(mtc_client_request_count)	发出的 API 请求总数
mtc_client_request_elapsed	API 请求延迟，根据请求类型排序
sum(mtc_client_request_elapsed)	API 请求的总延迟
sum(mtc_client_request_elapsed) / sum(mtc_client_request_count)	API 请求的平均延迟
mtc_client_request_elapsed / mtc_client_request_count	API 请求的平均延迟，按请求类型排序
cam_app_workload_migrations{status="running"} * 100	运行的迁移计数，乘以 100 可更轻松查看请求数

11.3.5. 使用 must-gather 工具

您可以使用 **must-gather** 工具来收集 MTC 自定义资源的日志、指标和相关信息。

must-gather 数据必须附加到所有客户案例。

您可以收集一小时或 24 小时内的数据，并使用 Prometheus 控制台查看数据。

先决条件

- 您必须使用具有 **cluster-admin** 角色的用户登录到 OpenShift Container Platform 集群。
- 已安装 OpenShift CLI (**oc**)。

流程

1. 进入存储 **must-gather** 数据的目录。
2. 为以下数据收集选项之一运行 **oc adm must-gather** 命令：
   - 要收集过去 24 小时的数据，请使用以下命令：

     ```
     $ oc adm must-gather --image=registry.redhat.io/rhmtc/openshift-migration-must-gather-rhel8:v1.8
     ```

     这个命令将数据保存为 **must-gather/must-gather.tar.gz** 文件。您可以将此文件上传到红帽客户门户网站中的支持问题单中。

   - 要收集过去 24 小时的数据，请使用以下命令：

```
$ oc adm must-gather --image=registry.redhat.io/rhmtc/openshift-migration-must-gather-rhel8:v1.8 -- /usr/bin/gather_metrics_dump
```

此操作可能需要很长时间。这个命令将数据保存为 **must-gather/metrics/prom_data.tar.gz** 文件。

11.3.6. 使用 Velero CLI 工具调试 Velero 资源

您可以调试 **Backup** 和 **Restore** 自定义资源(CR)并使用 Velero CLI 工具检索日志。

Velero CLI 工具比 OpenShift CLI 工具提供更详细的信息。

语法
使用 **oc exec** 命令运行 Velero CLI 命令：

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  <backup_restore_cr> <command> <cr_name>
```

Example

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  backup describe 0e44ae00-5dc3-11eb-9ca8-df7e5254778b-2d8ql
```

帮助选项
使用 **velero --help** 列出所有 Velero CLI 命令：

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  --help
```

describe 命令
使用 **velero describe** 命令检索与 **Backup** 或 **Restore** CR 关联的警告和错误概述：

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  <backup_restore_cr> describe <cr_name>
```

Example

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  backup describe 0e44ae00-5dc3-11eb-9ca8-df7e5254778b-2d8ql
```

velero describe 请求的输出中会显示以下类型的恢复错误和警告：

- **Velero**: 与 Velero 本身操作相关的信息列表，例如：与连接到云相关的信息，读取备份文件等
- **集群**：与备份和恢复集群范围的资源相关的消息列表
- **命名空间**：与备份或恢复存储在命名空间中资源相关的消息列表

这些类别中的一个或多个错误会导致 **Restore** 操作接收 **PartiallyFailed** 而不是 **Completed** 状态。警告不会造成完成状态的更改。

重要

- 对于特定于资源的错误，即 **Cluster** 和 **Namespaces** 错误，**restore describe --details** 输出包含一个资源列表，其中列出了 Velero 在恢复中成功的所有资源。对于具有此类错误的任何资源，请检查资源是否实际位于集群中。
- 如果存在 **Velero** 错误，但没有特定于资源的错误，在 **describe** 命令的输出中没有完成恢复，且没有恢复工作负载中的实际问题，但仔细验证恢复后应用程序。例如，如果输出包含 **PodVolumeRestore** 或节点代理相关的错误，请检查 **PodVolumeRestores** 和 **DataDownloads** 的状态。如果其中任何失败或仍在运行，则卷数据可能已被完全恢复。

logs 命令
使用 **velero logs** 命令检索 **Backup** 或 **Restore** CR 的日志：

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  <backup_restore_cr> logs <cr_name>
```

Example

```
$ oc -n openshift-migration exec deployment/velero -c velero -- ./velero \
  restore logs ccc7c2d0-6017-11eb-afab-85d0007f5a19-x4lbf
```

11.3.7. 调试部分迁移失败

您可以使用 Velero CLI 检查 **Restore** 自定义资源（CR）日志来调试部分迁移失败警告消息。

当 Velero 遇到没有导致迁移失败的问题时，会导致迁移部分失败。例如，缺少自定义资源定义（CRD），或者源集群和目标集群的 CRD 版本之间存在冲突，则迁移会完成，但不会在目标集群上创建 CR。

Velero 将问题作为部分失败记录，然后处理 **备份** CR 中的其他对象。

流程

1. 检查 **MigMigration** CR 的状态：

```
$ oc get migmigration <migmigration> -o yaml
```

输出示例

```
status:
  conditions:
  - category: Warn
    durable: true
    lastTransitionTime: "2021-01-26T20:48:40Z"
    message: 'Final Restore openshift-migration/ccc7c2d0-6017-11eb-afab-85d0007f5a19-
x4lbf: partially failed on destination cluster'
    status: "True"
    type: VeleroFinalRestorePartiallyFailed
  - category: Advisory
    durable: true
    lastTransitionTime: "2021-01-26T20:48:42Z"
```

```
    message: The migration has completed with warnings, please look at `Warn` conditions.
    reason: Completed
    status: "True"
    type: SucceededWithWarnings
```

2. 使用 Velero **describe** 命令检查 **Restore** CR 的状态：

```
$ oc -n {namespace} exec deployment/velero -c velero -- ./velero \
  restore describe <restore>
```

输**出示例**

```
Phase:  PartiallyFailed (run 'velero restore logs ccc7c2d0-6017-11eb-afab-85d0007f5a19-x4lbf' for more information)

Errors:
  Velero:     <none>
  Cluster:    <none>
  Namespaces:
    migration-example:  error restoring example.com/migration-example/migration-example: the server could not find the requested resource
```

3. 使用 Velero **logs** 命令检查 **Restore** CR 日志：

```
$ oc -n {namespace} exec deployment/velero -c velero -- ./velero \
  restore logs <restore>
```

输**出示例**

```
time="2021-01-26T20:48:37Z" level=info msg="Attempting to restore migration-example: migration-example" logSource="pkg/restore/restore.go:1107" restore=openshift-migration/ccc7c2d0-6017-11eb-afab-85d0007f5a19-x4lbf
time="2021-01-26T20:48:37Z" level=info msg="error restoring migration-example: the server could not find the requested resource" logSource="pkg/restore/restore.go:1170" restore=openshift-migration/ccc7c2d0-6017-11eb-afab-85d0007f5a19-x4lbf
```

Restore CR 会记录日志错误消息， **the server could not find the requested resource**，代表迁移部分失败的原因。

11.3.8. 使用 MTC 自定义资源进行故障排除

您可以检查以下 MTC 自定义资源（CR）来排除迁移失败的问题：

- **MigCluster**
- **MigStorage**
- **MigPlan**
- **BackupStorageLocation**
  BackupStorageLocation CR 包含一个 **migrationcontroller** 标签，用于标识创建 CR 的 MTC 实例：

```
    labels:
      migrationcontroller: ebe13bee-c803-47d0-a9e9-83f380328b93
```

- **VolumeSnapshotLocation**
  VolumeSnapshotLocation CR 包含一个 **migrationcontroller** 标签，用于标识创建 CR 的 MTC 实例：

```
    labels:
      migrationcontroller: ebe13bee-c803-47d0-a9e9-83f380328b93
```

- **MigMigration**
- **Backup**
  在目标集群中，MTC 将迁移的持久性卷（PV）的重新声明策略设置为 **Retain**。**Backup** CR 包含 **openshift.io/orig-reclaim-policy** 注解，用于指示原始重新声明策略。您可以手动恢复迁移 PV 的重新声明策略。
- **恢复**

流程

1. 列出 **openshift-migration** 命名空间中的 **MigMigration** CR:

```
$ oc get migmigration -n openshift-migration
```

   输**出示例**

```
NAME                                   AGE
88435fe0-c9f8-11e9-85e6-5d593ce65e10   6m42s
```

2. 检查 **MigMigration** CR:

```
$ oc describe migmigration 88435fe0-c9f8-11e9-85e6-5d593ce65e10 -n openshift-migration
```

   输出结果类似以下示例。

MigMigration 示例输**出**

```
name:         88435fe0-c9f8-11e9-85e6-5d593ce65e10
namespace:    openshift-migration
labels:       <none>
annotations:  touch: 3b48b543-b53e-4e44-9d34-33563f0f8147
apiVersion:  migration.openshift.io/v1alpha1
kind:         MigMigration
metadata:
  creationTimestamp:  2019-08-29T01:01:29Z
  generation:         20
  resourceVersion:    88179
  selfLink:           /apis/migration.openshift.io/v1alpha1/namespaces/openshift-
migration/migmigrations/88435fe0-c9f8-11e9-85e6-5d593ce65e10
  uid:                8886de4c-c9f8-11e9-95ad-0205fe66cbb6
spec:
  migPlanRef:
```

```
    name:        socks-shop-mig-plan
    namespace:   openshift-migration
  quiescePods:  true
  stage:        false
status:
  conditions:
    category:             Advisory
    durable:              True
    lastTransitionTime:  2019-08-29T01:03:40Z
    message:              The migration has completed successfully.
    reason:               Completed
    status:               True
    type:                 Succeeded
  phase:                  Completed
  startTimestamp:         2019-08-29T01:01:29Z
events:                   <none>
```

Velero 备份 CR #2 示例输出来描述 PV 数据

```
apiVersion: velero.io/v1
kind: Backup
metadata:
  annotations:
    openshift.io/migrate-copy-phase: final
    openshift.io/migrate-quiesce-pods: "true"
    openshift.io/migration-registry: 172.30.105.179:5000
    openshift.io/migration-registry-dir: /socks-shop-mig-plan-registry-44dd3bd5-c9f8-11e9-95ad-
0205fe66cbb6
    openshift.io/orig-reclaim-policy: delete
  creationTimestamp: "2019-08-29T01:03:15Z"
  generateName: 88435fe0-c9f8-11e9-85e6-5d593ce65e10-
  generation: 1
  labels:
    app.kubernetes.io/part-of: migration
    migmigration: 8886de4c-c9f8-11e9-95ad-0205fe66cbb6
    migration-stage-backup: 8886de4c-c9f8-11e9-95ad-0205fe66cbb6
    velero.io/storage-location: myrepo-vpzq9
  name: 88435fe0-c9f8-11e9-85e6-5d593ce65e10-59gb7
  namespace: openshift-migration
  resourceVersion: "87313"
  selfLink: /apis/velero.io/v1/namespaces/openshift-migration/backups/88435fe0-c9f8-11e9-85e6-
5d593ce65e10-59gb7
  uid: c80dbbc0-c9f8-11e9-95ad-0205fe66cbb6
spec:
  excludedNamespaces: []
  excludedResources: []
  hooks:
    resources: []
  includeClusterResources: null
  includedNamespaces:
  - sock-shop
  includedResources:
  - persistentvolumes
  - persistentvolumeclaims
  - namespaces
```

```
  - imagestreams
  - imagestreamtags
  - secrets
  - configmaps
  - pods
  labelSelector:
    matchLabels:
      migration-included-stage-backup: 8886de4c-c9f8-11e9-95ad-0205fe66cbb6
  storageLocation: myrepo-vpzq9
  ttl: 720h0m0s
  volumeSnapshotLocations:
  - myrepo-wv6fx
status:
  completionTimestamp: "2019-08-29T01:02:36Z"
  errors: 0
  expiration: "2019-09-28T01:02:35Z"
  phase: Completed
  startTimestamp: "2019-08-29T01:02:35Z"
  validationErrors: null
  version: 1
  volumeSnapshotsAttempted: 0
  volumeSnapshotsCompleted: 0
  warnings: 0
```

Velero 恢复 CR #2 示例输出来描述 Kubernetes 资源

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  annotations:
    openshift.io/migrate-copy-phase: final
    openshift.io/migrate-quiesce-pods: "true"
    openshift.io/migration-registry: 172.30.90.187:5000
    openshift.io/migration-registry-dir: /socks-shop-mig-plan-registry-36f54ca7-c925-11e9-825a-
06fa9fb68c88
  creationTimestamp: "2019-08-28T00:09:49Z"
  generateName: e13a1b60-c927-11e9-9555-d129df7f3b96-
  generation: 3
  labels:
    app.kubernetes.io/part-of: migration
    migmigration: e18252c9-c927-11e9-825a-06fa9fb68c88
    migration-final-restore: e18252c9-c927-11e9-825a-06fa9fb68c88
  name: e13a1b60-c927-11e9-9555-d129df7f3b96-gb8nx
  namespace: openshift-migration
  resourceVersion: "82329"
  selfLink: /apis/velero.io/v1/namespaces/openshift-migration/restores/e13a1b60-c927-11e9-9555-
d129df7f3b96-gb8nx
  uid: 26983ec0-c928-11e9-825a-06fa9fb68c88
spec:
  backupName: e13a1b60-c927-11e9-9555-d129df7f3b96-sz24f
  excludedNamespaces: null
  excludedResources:
  - nodes
  - events
  - events.events.k8s.io
```

```
  - backups.velero.io
  - restores.velero.io
  - resticrepositories.velero.io
  includedNamespaces: null
  includedResources: null
  namespaceMapping: null
  restorePVs: true
status:
  errors: 0
  failureReason: ""
  phase: Completed
  validationErrors: null
  warnings: 15
```

11.4. 常见问题和关注

本节介绍在迁移过程中可能导致问题的常见问题。

11.4.1. 直接卷迁移未完成

如果直接卷迁移未完成，则目标集群可能没有与源集群相同的 **node-selector** 注解。

MTC 在迁移命名空间时会保留所有注解，以保持安全性上下文约束和调度要求。在直接卷迁移过程中，MTC 在从源集群迁移的命名空间中在目标集群上创建 Rsync 传输 pod。如果目标集群命名空间没有与源集群命名空间相同的注解，则无法调度 Rsync 传输 pod。Rsync pod 处于 **Pending** 状态。

您可以执行以下步骤识别并解决这个问题。

流程

1. 检查 **MigMigration** CR 的状态：

```
$ oc describe migmigration <pod> -n openshift-migration
```

输出包括以下状态消息：

输**出示例**

```
Some or all transfer pods are not running for more than 10 mins on destination cluster
```

2. 在源集群中，获取迁移的命名空间的详情：

```
$ oc get namespace <namespace> -o yaml 1
```

1 指定迁移的命名空间。

3. 在目标集群中，编辑迁移的命名空间：

```
$ oc edit namespace <namespace>
```

4. 将缺少的 **openshift.io/node-selector** 注解添加到迁移的命名空间中，如下例所示：

```
apiVersion: v1
kind: Namespace
metadata:
  annotations:
    openshift.io/node-selector: "region=east"
...
```

5. 再次运行迁移计划。

11.4.2. 错误信息和解决方案

本节论述了您可能会在 Migration Toolkit for Containers（MTC）中遇到的常见错误消息，以及如何解决其底层原因。

11.4.2.1. 首次访问 MTC 控制台时显示的 CA 证书错误

如果在第一次尝试访问 MTC 控制台时显示 **CA 证书错误**信息，则可能的原因是在一个集群中使用自签名的 CA 证书。

要解决这个问题，进入出错信息中显示的 **oauth-authorization-server** URL 并接受证书。要永久解决这个问题，将证书添加到网页浏览器的信任存储中。

如果您接受证书后显示 **Unauthorized** 信息，进入 MTC 控制台并刷新网页。

11.4.2.2. MTC 控制台中的 OAuth 超时错误

如果在接受自签名证书后，MTC 控制台中显示 **connection has timed out**，其原因可能是：

- 对 OAuth 服务器的网络访问中断
- 对 OpenShift Container Platform 控制台的网络访问中断
- 代理配置中阻断了对 **oauth-authorization-server** URL 的访问。详情请查看因为 OAuth 超时错误而无法访问 MTC 控制台。

要确定超时的原因：

- 使用浏览器 web 检查器检查 MTC 控制台网页。
- 检查 **Migration UI** pod 日志中的错误。

11.4.2.3. 由未知颁发机构签名的证书错误

如果您使用自签名证书来保护集群或 MTC 的 Migration Toolkit 的复制仓库的安全，则证书验证可能会失败，并显示以下错误消息： **Certificate signed by unknown authority**。

您可以创建自定义 CA 证书捆绑包文件，并在添加集群或复制存储库时将其上传到 MTC web 控制台。

流程

从远程端点下载 CA 证书，并将其保存为 CA 捆绑包文件：

```
$ echo -n | openssl s_client -connect <host_FQDN>:<port> \ 1
  | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > <ca_bundle.cert> 2
```

1 指定端点的主机 FQDN 和端口，如 **api.my-cluster.example.com:6443**。

2 指定 CA 捆绑包文件的名称。

11.4.2.4. 在 Velero pod 日志中有备份存储位置错误

如果 **Velero Backup** 自定义资源包含对不存在的备份存储位置（BSL）的引用，**Velero** pod 日志可能会显示以下错误消息：

```
$ oc logs <Velero_Pod> -n openshift-migration
```

输出示例

```
level=error msg="Error checking repository for stale locks" error="error getting backup storage
location: BackupStorageLocation.velero.io \"ts-dpa-1\" not found" error.file="/remote-
source/src/github.com/vmware-tanzu/velero/pkg/restic/repository_manager.go:259"
```

您可以忽略这些错误消息。缺少 BSL 不会导致迁移失败。

11.4.2.5. Velero pod 日志中的 Pod 卷备份超时错误

如果因为 Restic 超时造成迁移失败，以下错误会在 **Velero** pod 日志中显示。

```
level=error msg="Error backing up item" backup=velero/monitoring error="timed out waiting for all
PodVolumeBackups to complete"
error.file="/go/src/github.com/heptio/velero/pkg/restic/backupper.go:165"
error.function="github.com/heptio/velero/pkg/restic.(*backupper).BackupPodVolumes" group=v1
```

restic_timeout 的默认值为一小时。您可以为大型迁移增加这个参数值，请注意，高的值可能会延迟返回出错信息。

流程

1. 在 OpenShift Container Platform web 控制台中导航至 **Operators → Installed Operators**。
2. 点 **Migration Toolkit for Containers Operator**。
3. 在 **MigrationController** 标签页中点 **migration-controller**。
4. 在 **YAML** 标签页中，更新以下参数值：

```
spec:
  restic_timeout: 1h 1
```

1 有效单元是 **h**（小时）、**m**（分钟）和 **s**（秒），例如 **3h30m15s**。

5. 点击 **Save**。

11.4.2.6. MigMigration 自定义资源中的 Restic 验证错误

如果迁移使用文件系统数据复制方法的持久性卷时数据验证失败，在 **MigMigration** CR 中会显示以下错误。

输**出示例**

```
status:
  conditions:
  - category: Warn
    durable: true
    lastTransitionTime: 2020-04-16T20:35:16Z
    message: There were verify errors found in 1 Restic volume restores. See restore `<registry-example-migration-rvwcm>`
      for details 1
    status: "True"
    type: ResticVerifyErrors 2
```

1 错误消息指定了 **Restore** CR 名称。

2 **ResticVerifyErrors** 是一个包括验证错误的一般错误警告类型。

注意

数据验证错误不会导致迁移过程失败。

您可以检查 **Restore** CR，以识别数据验证错误的来源。

流程

1. 登录到目标集群。
2. 查看 **Restore** CR：

```
$ oc describe <registry-example-migration-rvwcm> -n openshift-migration
```

输出会标识出带有 **PodVolumeRestore** 错误的持久性卷。

输**出示例**

```
status:
  phase: Completed
  podVolumeRestoreErrors:
  - kind: PodVolumeRestore
    name: <registry-example-migration-rvwcm-98t49>
    namespace: openshift-migration
  podVolumeRestoreResticErrors:
  - kind: PodVolumeRestore
    name: <registry-example-migration-rvwcm-98t49>
    namespace: openshift-migration
```

3. 查看 **PodVolumeRestore** CR:

```
$ oc describe <migration-example-rvwcm-98t49>
```

输出中标识了记录错误的 **Restic** pod。

输**出示例**

```
completionTimestamp: 2020-05-01T20:49:12Z
errors: 1
resticErrors: 1
...
resticPod: <restic-nr2v5>
```

4. 查看 **Restic** pod 日志以查找错误：

```
$ oc logs -f <restic-nr2v5>
```

11.4.2.7. 从启用了 root_squash 的 NFS 存储中迁移时的 Restic 权限错误

如果您要从 NFS 存储中迁移数据，并且启用了 **root_squash**，**Restic** 会映射到 **nfsnobody**，且没有执行迁移的权限。**Restic** pod 日志中显示以下错误。

输**出示例**

```
backup=openshift-migration/<backup_id> controller=pod-volume-backup error="fork/exec
/usr/bin/restic: permission denied" error.file="/go/src/github.com/vmware-
tanzu/velero/pkg/controller/pod_volume_backup_controller.go:280"
error.function="github.com/vmware-tanzu/velero/pkg/controller.
(*podVolumeBackupController).processBackup"
logSource="pkg/controller/pod_volume_backup_controller.go:280" name=<backup_id>
namespace=openshift-migration
```

您可以通过为 Restic 创建补充组并将组 ID 添加到 **MigrationController** CR 清单来解决这个问题。

流程

1. 在 NFS 存储上为 Restic 创建补充组。
2. 在 NFS 目录上设置 **setgid** 位，以便继承组所有权。
3. 将 **restic_supplemental_groups** 参数添加到源和目标集群上的 **MigrationController** CR 清单：

```
spec:
  restic_supplemental_groups: <group_id> 1
```

1 指定补充组 ID。

4. 等待 **Restic** pod 重启，以便应用更改。

11.4.3. 使用 spc_t 在 OpenShift Container Platform 上运行的工作负载自动应用 Skip SELinux 重新标记临时解决方案

当尝试使用 Migration Toolkit for Containers (MTC)迁移命名空间以及与之关联的大量卷时，**rsync-server** 可能会冻结，且没有提供用于进一步排除此问题的信息。

11.4.3.1. 诊断 Skip SELinux 重新标记临时解决方案

在 kubelet 日志中搜索 **Unable to attach or mount volumes for pod…timed out waiting for the condition** 错误，它来自为 Direct Volume Migration (DVM) 运行 **rsync-server** 的节点。

kubelet 日志示例

```
kubenswrapper[3879]: W0326 16:30:36.749224    3879 volume_linux.go:49] Setting volume ownership for /var/lib/kubelet/pods/8905d88e-6531-4d65-9c2a-eff11dc7eb29/volumes/kubernetes.io~csi/pvc-287d1988-3fd9-4517-a0c7-22539acd31e6/mount and fsGroup set. If the volume has a lot of files then setting volume ownership could be slow, see https://github.com/kubernetes/kubernetes/issues/69699

kubenswrapper[3879]: E0326 16:32:02.706363    3879 kubelet.go:1841] "Unable to attach or mount volumes for pod; skipping pod" err="unmounted volumes=[8db9d5b032dab17d4ea9495af12e085a], unattached volumes=[crane2-rsync-server-secret 8db9d5b032dab17d4ea9495af12e085a kube-api-access-dlbd2 crane2-stunnel-server-config crane2-stunnel-server-secret crane2-rsync-server-config]: timed out waiting for the condition" pod="caboodle-preprod/rsync-server"

kubenswrapper[3879]: E0326 16:32:02.706496    3879 pod_workers.go:965] "Error syncing pod, skipping" err="unmounted volumes=[8db9d5b032dab17d4ea9495af12e085a], unattached volumes=[crane2-rsync-server-secret 8db9d5b032dab17d4ea9495af12e085a kube-api-access-dlbd2 crane2-stunnel-server-config crane2-stunnel-server-secret crane2-rsync-server-config]: timed out waiting for the condition" pod="caboodle-preprod/rsync-server" podUID=8905d88e-6531-4d65-9c2a-eff11dc7eb29
```

11.4.3.2. 使用 Skip SELinux 重新标记临时解决方案解决

要解决这个问题，使用 **MigrationController** 自定义资源(CR)在源和目标 **MigClusters** 中将 **migration_rsync_super_privileged** 参数设置为 **true**。

MigrationController CR 示例

```
apiVersion: migration.openshift.io/v1alpha1
kind: MigrationController
metadata:
  name: migration-controller
  namespace: openshift-migration
spec:
  migration_rsync_super_privileged: true (1)
  azure_resource_group: ""
  cluster_name: host
  mig_namespace_limit: "10"
  mig_pod_limit: "100"
  mig_pv_limit: "100"
  migration_controller: true
  migration_log_reader: true
  migration_ui: true
  migration_velero: true
  olm_managed: true
  restic_timeout: 1h
  version: 1.8.3
```

(1) **migration_rsync_super_privileged** 参数的值指示是否将 Rsync Pod 作为 *超级特权容器* 运行 (**spc_t selinux context**)。有效设置为 **true** 或 **false**。

11.5. 回滚一个迁移

您可以使用 MTC web 控制台或 CLI 回滚迁移。

您还可以手动回滚迁移。

11.5.1. 使用 MTC web 控制台回滚迁移

您可以使用 Migration Toolkit for Containers（MTC）web 控制台回滚迁移。

注意

以下资源保留在迁移的命名空间中，以便在直接卷迁移 (DVM) 失败后进行调试：

- 配置映射（源和目标集群）
- **Secret** 对象（源和目标集群）
- **Rsync** CR（源集群）

这些资源不会影响回滚。您可以手动删除它们。

如果您稍后成功运行相同的迁移计划，则会自动删除失败迁移中的资源。

如果应用程序在迁移失败时停止，您必须回滚迁移，以防止持久性卷中的数据崩溃。

如果应用程序在迁移过程中没有停止，则不需要回滚，因为原始应用程序仍然在源集群中运行。

流程

1. 在 MTC web 控制台中点 **Migration Plan**。
2. 点击迁移计划  旁边的 Options 菜单，并在 **Migration** 下选择 **Rollback**。
3. 点 **Rollback** 并等待回滚完成。
   在迁移计划详情中会显示 **Rollback succeeded**。
4. 验证源集群的 OpenShift Container Platform Web 控制台中是否成功回滚：
   a. 点 **Home → Projects**。
   b. 点迁移的项目查看其状态。
   c. 在 **Routes** 部分，点击 **Location** 验证应用程序是否正常运行。
   d. 点 **Workloads → Pods** 来验证 pod 是否在迁移的命名空间中运行。
   e. 点 **Storage → Persistent volumes** 确认正确置备了被迁移的持久性卷。

11.5.2. 使用命令行界面回滚迁移

您可以通过从命令行界面创建 **MigMigration** 自定义资源（CR）来回滚迁移。

注意

以下资源保留在迁移的命名空间中，以便在直接卷迁移 (DVM) 失败后进行调试：

- 配置映射（源和目标集群）
- **Secret** 对象（源和目标集群）
- **Rsync** CR（源集群）

这些资源不会影响回滚。您可以手动删除它们。

如果您稍后成功运行相同的迁移计划，则会自动删除失败迁移中的资源。

如果应用程序在迁移失败时停止，您必须回滚迁移，以防止持久性卷中的数据崩溃。

如果应用程序在迁移过程中没有停止，则不需要回滚，因为原始应用程序仍然在源集群中运行。

流程

1. 根据以下示例创建一个 **MigMigration** CR：

```
$ cat << EOF | oc apply -f -
apiVersion: migration.openshift.io/v1alpha1
kind: MigMigration
metadata:
  labels:
    controller-tools.k8s.io: "1.0"
  name: <migmigration>
  namespace: openshift-migration
spec:
...
  rollback: true
...
  migPlanRef:
    name: <migplan> 1
    namespace: openshift-migration
EOF
```

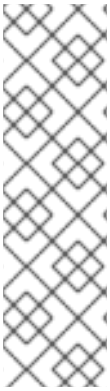
1 指定关联的 **MigPlan** CR 的名称。

2. 在 MTC web 控制台中，验证迁移的项目资源是否已从目标集群中移除。
3. 验证迁移的项目资源是否存在于源集群中，并且应用程序是否正在运行。

11.5.3. 手动回滚迁移

您可以通过删除 **stage** pod 并取消静止应用程序来手动回滚失败的迁移。

如果您成功运行相同的迁移计划，则会自动删除失败迁移中的资源。



注意

在直接卷迁移失败 (DVM) 后，以下资源会保留在迁移的命名空间中：

- 配置映射（源和目标集群）
- **Secret** 对象（源和目标集群）
- **Rsync** CR（源集群）

这些资源不会影响回滚。您可以手动删除它们。

流程

1. 删除所有集群中的 **stage** pod：

```
$ oc delete $(oc get pods -l migration.openshift.io/is-stage-pod -n <namespace>) 1
```

1 **MigPlan** CR 中指定的命名空间。

2. 通过将副本扩展到其预迁移编号，在源集群中取消静默应用程序：

```
$ oc scale deployment <deployment> --replicas=<premigration_replicas>
```

Deployment CR 中的 **migration.openshift.io/preQuiesceReplicas** 注解显示预迁移副本数：

```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  annotations:
    deployment.kubernetes.io/revision: "1"
    migration.openshift.io/preQuiesceReplicas: "1"
```

3. 验证应用程序 pod 是否在源集群中运行：

```
$ oc get pod -n <namespace>
```

其他资源

- 使用 Web 控制台从集群中删除 Operator